(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－73424
（P2002－73424A）
(43)公開日　平成14年３月12日(2002.3.12)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｆ	５Ｂ０１７
Ｇ０６Ｋ　17/00		Ｇ０６Ｋ　17/00	Ｌ	５Ｂ０３５
19/00		19/00	Ｔ	５Ｂ０５８
Ｈ０４Ｑ　7/38		Ｈ０４Ｂ　7/26	１０９Ｓ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７３Ｄ	５Ｋ０６７

審査請求　未請求　請求項の数57　ＯＬ　（全 49 頁）　最終頁に続く

(21)出願番号　特願2000－262445(P2000－262445)

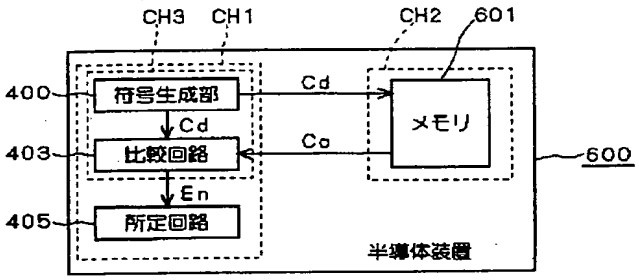
(22)出願日　平成12年８月31日(2000.8.31)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　前田　茂伸
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100089233
弁理士　吉田　茂明　（外２名）

最終頁に続く

(54)【発明の名称】　半導体装置、端末装置および通信方法

(57)【要約】
【課題】　半導体基板を取り替えてなされる半導体装置の応用機器の不正使用に対する技術的障壁を高める。
【解決手段】　符号生成部４００は、半導体基板ＣＨ１（またはＣＨ３）に固有の識別符号Ｃｄを生成する。別の半導体基板ＣＨ２に形成されたメモリ６０１は、識別符号Ｃｄを記憶符号Ｃｏとして記憶する。識別符号Ｃｄは、半導体装置６００が製品として出荷されるときに、符号生成部４００からメモリ６０１へ書き込まれる。比較回路４０３は、識別符号Ｃｄと記憶符号Ｃｏとを比較し、これら双方が互いに一致しないときには、所定回路４０５の一部の動作を停止する。



1

【特許請求の範囲】

【請求項１】　少なくとも一つの半導体基板の各々に形成され、その半導体基板に固有の識別符号を生成する符号生成部と、

前記識別符号の各々ごとに、対応する半導体基板とは別の半導体基板に形成され、対応する識別符号に一致する符号を記憶符号として記憶するメモリと、を備える半導体装置。

【請求項２】　前記メモリが、前記記憶符号を記憶するＯＴＰＲＯＭを備える、請求項１に記載の半導体装置。

【請求項３】　前記符号生成部が、

半導体素子と、

前記半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより、前記識別符号を生成し、出力する符号化回路と、を備える、請求項１または請求項２に記載の半導体装置。

【請求項４】　前記半導体素子が多結晶体を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する、請求項３に記載の半導体装置。

【請求項５】　前記符号生成部が、前記識別符号を記憶するＯＴＰＲＯＭを備える、請求項１または請求項２に記載の半導体装置。

【請求項６】　前記識別符号の各々ごとに、前記識別符号と、対応する前記記憶符号とを比較し、これら双方が一致するか否かを判定し、その結果を表現する判定信号を出力する比較回路を、さらに備える、請求項１ないし請求項５のいずれかに記載の半導体装置。

【請求項７】　前記比較回路が、比較対象とする識別符号に対応する前記半導体基板に形成されている、請求項６に記載の半導体装置。

【請求項８】　前記識別符号の各々ごとに、対応する前記半導体基板に形成された鍵生成部、暗号化回路および復号化回路を、さらに備え、

前記鍵生成部は、対応する前記半導体基板に固有である暗号化のための鍵を生成し、

前記暗号化回路は、対応する前記半導体基板に形成された前記符号生成部が生成する前記識別符号を、対応する前記鍵にもとづいて暗号化し、暗号化された形式で対応する前記メモリへ伝え、

対応する前記メモリは、前記暗号化回路が出力する暗号化された形式での前記識別符号を、暗号化された形式での前記記憶符号として記憶し、

前記復号化回路は、対応する前記メモリに記憶される暗号化された前記記憶符号を、対応する前記鍵にもとづいて復号化し、

前記比較回路は、対応する前記符号化回路が生成する前記識別符号と、対応する前記復号化回路が生成する復号化された前記記憶符号とを比較する、請求項７に記載の

2

半導体装置。

【請求項９】　前記鍵生成部が、

別の半導体素子と、

前記別の半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより、前記鍵を生成し、出力する別の符号化回路と、を備える、請求項８に記載の半導体装置。

【請求項１０】　前記別の半導体素子が多結晶体を有しており、前記別の半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する、請求項９に記載の半導体装置。

【請求項１１】　前記鍵生成部が、前記鍵を記憶するＯＴＰＲＯＭを備える、請求項８に記載の半導体装置。

【請求項１２】　前記識別符号の各々ごとに、対応する前記半導体基板に形成され、対応する前記符号化回路が生成した前記識別符号の、対応する前記メモリへの送出と、対応する前記メモリに記憶される前記記憶符号の前記比較回路への入力とを、排他的に行うスイッチ回路を、さらに備える、請求項７ないし請求項１１のいずれかに記載の半導体装置。

【請求項１３】　前記識別符号の各々に対応した前記判定信号に依存して選択的に動作または非動作となる回路部分を含む所定回路を、さらに備える、請求項６ないし請求項１２のいずれかに記載の半導体装置。

【請求項１４】　前記所定回路が、前記比較回路が形成されている前記少なくとも一つの半導体基板の一つに形成されている、請求項１３に記載の半導体装置。

【請求項１５】　前記少なくとも一つの半導体基板の個数が単一である、請求項１ないし請求項１４のいずれかに記載の半導体装置。

【請求項１６】　前記少なくとも一つの半導体基板の個数が２個であり、

前記識別符号の各々ごとに、対応する前記符号生成部と前記メモリは、互いに前記２個の半導体基板の一方と他方とに形成されている、請求項１ないし請求項１４のいずれかに記載の半導体装置。

【請求項１７】　半導体素子と当該半導体素子の電気的特性のばらつきに由来して値がばらつくように前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより暗号化のための鍵を生成し、出力する符号化回路とを備える鍵生成部と、

前記鍵にもとづいて送信データを暗号化する暗号化回路と、

前記鍵にもとづいて受信データを復号化する復号化回路と、を備える端末装置。

【請求項１８】　前記符号化回路と前記復号化回路とが本体部に組み込まれており、

前記鍵生成部が、前記本体部に脱着自在の補助部に組み込まれている、請求項１７に記載の端末装置。

【請求項１９】　前記補助部がＩＣカードである、請求項１８に記載の端末装置。

【請求項２０】　前記半導体素子が多結晶体を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する、請求項１７ないし請求項１９のいずれかに記載の端末装置。

【請求項２１】　請求項１３または請求項１４に記載の半導体装置を備え、

前記所定回路が、外部との間で信号を送信および受信する通信回路であって、前記判定信号の各々が前記識別符号の少なくとも一つと対応する前記記憶符号との間の不一致を示すときには、送信または受信の少なくとも一方を停止する端末装置。

【請求項２２】　請求項６ないし請求項１２のいずれかに記載の半導体装置と、

外部との間で信号を送信および受信する通信回路と、を備え、

前記通信回路は、前記信号の一部として前記判定信号の各々を前記外部へ送信する端末装置。

【請求項２３】　請求項１ないし請求項５のいずれかに記載の半導体装置と、

外部との間で信号を送信および受信する通信回路と、を備え、

前記通信回路は、前記信号の一部として前記識別符号の各々と前記記憶符号の各々とを前記外部へ送信する端末装置。

【請求項２４】　前記少なくとも一つの半導体基板の個数が単一であって、

前記符号生成部の各々と前記通信回路とが本体部に組み込まれており、

前記メモリの各々が前記本体部に脱着自在の補助部に組み込まれている、請求項２３に記載の端末装置。

【請求項２５】　前記本体部には、

暗号化のための第１鍵を生成する第１鍵生成部と、

前記符号生成部が生成する前記識別符号を、前記第１鍵にもとづいて暗号化する第１暗号化回路と、がさらに組み込まれており、

前記補助部には、

暗号化のための第２鍵を生成する第２鍵生成部と、

前記メモリが記憶する前記記憶符号を、前記第２鍵にもとづいて暗号化する第２暗号化回路と、がさらに組み込まれており、

前記第１暗号化回路は、前記第２暗号化回路が暗号化した前記記憶符号をも、前記第１鍵にもとづいて暗号化し、

前記通信回路は、前記第１暗号化回路で暗号化された形式で、前記識別符号および前記記憶符号を前記外部へ送信する、請求項２４に記載の端末装置。

【請求項２６】　前記第１鍵生成部と前記第１暗号化回路とが、前記符号化回路が形成された前記半導体基板に

形成されている、請求項２５に記載の端末装置。

【請求項２７】　前記第２鍵生成部と前記第２暗号化回路とが、前記メモリが形成された前記半導体基板に形成されている、請求項２５または請求項２６に記載の端末装置。

【請求項２８】　前記本体部が、充電可能な電池を備えており、

前記補助部が、前記本体部に装着されることにより前記電池を充電する充電器である、請求項２４ないし請求項２７のいずれかに記載の端末装置。

【請求項２９】　前記補助部がＩＣカードであり、

前記本体部と前記補助部の各々には、前記補助部から前記本体部への符号の伝送を無線で媒介するための通信インタフェースが、さらに組み込まれている、請求項２４ないし請求項２７のいずれかに記載の端末装置。

【請求項３０】　前記通信回路が、前記少なくとも一つの半導体基板の一つに前記符号生成部とともに形成されている、請求項２２ないし請求項２９のいずれかに記載の端末装置。

【請求項３１】　通信事業者設備を媒介した無線通信を行う通信回路と、前記通信事業者設備を媒介しない無線通信網を形成することにより無線通信を行う無線通信網回路と、を備える端末装置。

【請求項３２】　前記通信回路と前記無線通信網回路との間での通信信号の経路の接続と切断とを選択自在に実行することにより、前記無線通信網を通じての前記端末装置の使用者と他者との間の通信と、前記無線通信網を通じての前記端末装置の使用者以外の複数の他者どうしの通信の中継と、を選択自在に実現する切替回路を、さらに備える、請求項３１に記載の端末装置。

【請求項３３】　暗号化のための鍵を生成する鍵生成部と、

前記通信信号の中で前記通信回路から前記無線通信網回路へ送られる送信信号を前記鍵にもとづいて暗号化する暗号化回路と、

前記通信信号の中で前記無線通信網回路から前記通信回路へ送られる受信信号を前記鍵にもとづいて復号化する復号化回路と、をさらに備え、

前記鍵生成部が、

前記端末装置を識別するための符号を生成する符号生成部と、

前記符号生成部が生成する前記符号と、前記無線通信網回路を通じて通信相手から送られる別の符号とにもとづいて、前記使用者と前記通信相手との間で共通に使用可能な共通鍵を算出する鍵演算部と、を備える、請求項３２に記載の端末装置。

【請求項３４】　前記符号生成部が、

半導体素子と、

前記半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタ

5

ル形式の信号へ変換することにより、前記符号を生成し、出力する符号化回路と、を備える、請求項３３に記載の端末装置。

【請求項３５】　前記半導体素子が多結晶体を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する、請求項３４に記載の端末装置。

【請求項３６】　前記符号生成部が、前記符号を記憶するＯＴＰＲＯＭを備える、請求項３３に記載の端末装置。

【請求項３７】　前記通信信号の中で前記無線通信網回路から前記通信回路へ送られる受信信号の経路に介挿された第１および第２ミキサを、さらに備え、

前記第１ミキサは、前記通信回路が受信した受信信号を復調し、

前記第２ミキサは、復調された前記受信信号を前記通信回路の周波数帯域内の周波数を有する搬送波を用いて変調する、請求項３２ないし請求項３６のいずれかに記載の端末装置。

【請求項３８】　事業者設備と請求項２２に記載の端末装置とが相互に通信を行う通信方法であって、

(a)前記端末装置が、前記判定信号の各々を前記事業者設備へ送信する工程と、

(b)前記事業者設備が、受信した前記判定信号の各々が、前記識別符号の各々と対応する前記記憶符号との一致を示すという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備える通信方法。

【請求項３９】　事業者設備と請求項２３に記載の端末装置とが相互に通信を行う通信方法であって、

(a)前記端末装置が、前記識別符号の各々と前記記憶符号の各々を前記事業者設備へ送信する工程と、

(b)前記事業者設備が、受信した前記識別符号の各々を対応する前記記憶符号と比較し、一致するか否かを判定する工程と、

(c)前記事業者設備が、前記工程(b)において前記識別符号の各々が対応する前記記憶符号に一致すると判定したという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備える通信方法。

【請求項４０】　(e)前記事業者設備が、受信した前記識別符号の各々と前記記憶符号の各々を記録する工程を、さらに備える、請求項３９に記載の通信方法。

【請求項４１】　前記工程(c)において、前記事業者設備は、前記認証を行わない場合には、受信した前記識別符号の各々と前記記憶符号の各々を記録する、請求項３９に記載の通信方法。

【請求項４２】　(a)事業者設備が、請求項２４に記載

6

の端末装置の前記識別符号を得て、第１登録符号として記憶する工程と、

(b)前記事業者設備が、前記端末装置の前記記憶符号を得て、第２登録符号として記憶する工程と、

(c)前記工程(a)および(b)の後に、前記事業者設備と前記端末装置とが相互に通信を行う通信工程と、を備え、

当該通信工程(c)は、

(c-1)前記補助部が前記本体部に装着されていないときに実行される第１通信工程と、

(c-2)前記補助部が前記本体部に装着されているときに実行される第２通信工程と、を備え、

前記第１通信工程(c-1)は、

(c-1-1)前記端末装置が、前記識別符号を前記事業者設備へ送信する工程と、

(c-1-2)前記事業者設備が、受信した前記識別符号と前記第１登録符号とを比較し、これら双方が一致するか否かを判定する工程と、

(c-1-3)前記事業者設備が、前記工程(c-1-2)で前記双方が一致すると判定したという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備え、

前記第２通信工程(c-2)は、

(c-2-1)前記端末装置が、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、

(c-2-2)前記事業者設備が、受信した前記識別符号と前記第１登録符号とを比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号と前記第２登録符号とを比較し、これら双方が一致するか否かを判定する工程と、

(c-2-3)前記事業者設備が、前記工程(c-2-2)の２つの判定のいずれにおいても一致するとの判定が得られたという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの高位の認証を行い、前記条件が充足されなければ、前記高位の認証を行わない高位認証工程と、を備える通信方法。

【請求項４３】　前記工程(b)では、前記補助部が前記本体部に装着された状態で前記事業者設備と前記端末装置とが通信を行うことにより、事業者設備が、前記端末装置の前記記憶符号を得る、請求項４２に記載の通信方法。

【請求項４４】　前記工程(c)が、

(c-3)前記補助部が前記本体部に装着されているときに実行され、前記第２登録符号の変更を行う変更工程を、さらに備え、

前記変更工程(c-3)は、

(c-3-1)前記端末装置が、前記変更の意志を表現する要求信号とともに、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、

(c-3-2)前記事業者設備が、受信した前記識別符号と前

記第１登録符号とを比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号と前記第２登録符号とを比較し、これら双方が一致するか否かを判定する工程と、

(c-3-3)前記事業者設備が、前記工程(c-3-2)の２つの判定のいずれにおいても一致するとの判定結果を得たときに限って、前記変更を許可する工程と、

(c-3-4)前記工程(c-3-3)の後に、前記端末装置の前記補助部を交換し、交換後の補助部を前記本体部へ装着する工程と、

(c-3-5)前記端末装置が、前記工程(c-3-4)の後に、前記識別符号と交換後の前記補助部にもとづく変更後の前記記憶符号とを前記事業者設備へ送信する工程と、

(c-3-6)前記事業者設備が、前記工程(c-3-3)で前記変更を許可した場合に限って、受信した変更後の前記記憶符号で前記第２登録符号を更新する工程と、を備える、請求項４２または請求項４３に記載の通信方法。

【請求項４５】　(a)事業者設備が、請求項２５に記載の端末装置の前記識別符号および前記第１鍵を得て、それぞれ第１登録符号および登録鍵として記憶する工程と、

(b)前記事業者設備が、前記端末装置の前記第２鍵で暗号化された前記記憶符号を得て、第２登録符号として記憶する工程と、

(c)前記工程(a)および(b)の後に、前記事業者設備と前記端末装置とが相互に通信を行う通信工程と、を備え、

当該通信工程(c)は、

(c-1)前記補助部が前記本体部に装着されていないときに実行される第１通信工程と、

(c-2)前記補助部が前記本体部に装着されているときに実行される第２通信工程と、を備え、

前記第１通信工程(c-1)は、

(c-1-1)前記端末装置が、前記第１暗号化回路で暗号化された形式で、前記識別符号を前記事業者設備へ送信する工程と、

(c-1-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第１登録符号と比較し、これら双方が一致するか否かを判定する工程と、

(c-1-3)前記事業者設備が、前記工程(c-1-2)で前記双方が一致すると判定したという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備え、

前記第２通信工程(c-2)は、

(c-2-1)前記端末装置が、前記第１暗号化回路で暗号化された形式で、前記識別符号および記憶符号を前記事業者設備へ送信する工程と、

(c-2-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第１登録符号と比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号を前記登録鍵にもとづいて復号化した上で、前記第２登録符号と比較し、これら双方が一致するか否かを判定する工程と、

(c-2-3)前記事業者設備が、前記工程(c-2-2)の２つの判定のいずれにおいても一致するとの判定が得られたという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの高位の認証を行い、前記条件が充足されなければ、前記高位の認証を行わない高位認証工程と、を備える通信方法。

【請求項４６】　前記工程(b)では、前記補助部が前記本体部に装着された状態で前記事業者設備と前記端末装置とが通信を行うことにより、事業者設備が、前記端末装置の前記第２鍵で暗号化された前記記憶符号を得る、請求項４５に記載の通信方法。

【請求項４７】　前記工程(c)が、

(c-3)前記補助部が前記本体部に装着されているときに実行され、前記第２登録符号の変更を行う変更工程を、さらに備え、

前記変更工程(c-3)は、

(c-3-1)前記端末装置が、前記変更の意志を表現する要求信号とともに、前記第１暗号化回路で暗号化された形式で、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、

(c-3-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第１登録符号と比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号を前記登録鍵にもとづいて復号化した上で、前記第２登録符号と比較し、これら双方が一致するか否かを判定する工程と、

(c-3-3)前記事業者設備が、前記工程(c-3-2)の２つの判定のいずれにおいても一致するとの判定結果を得たときに限って、前記変更を許可する工程と、

(c-3-4)前記工程(c-3-3)の後に、前記端末装置の前記補助部を交換し、交換後の補助部を前記本体部へ装着する工程と、

(c-3-5)前記端末装置が、前記工程(c-3-4)の後に、前記第１暗号化回路で暗号化された形式で、前記識別符号と交換後の前記補助部にもとづく変更後の前記記憶符号とを前記事業者設備へ送信する工程と、

(c-3-6)前記事業者設備が、前記工程(c-3-3)で前記変更を許可した場合に限って、受信した変更後の前記記憶符号を前記登録鍵にもとづいて復号化することにより得られる符号で、前記第２登録符号を更新する工程と、を備える、請求項４５または請求項４６に記載の通信方法。

【請求項４８】　前記高位認証工程において、前記事業者設備は、前記高位の認証を行わない場合には、前記工程(c-2-2)で各登録符号との比較の対象とされた各符号を記録する、請求項４２ないし請求項４７のいずれかに記載の通信方法。

9

【請求項４９】　前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合には、それ以前の通信に対する通信料金を、裏付けられたものとして記録する、請求項４２ないし請求項４８のいずれかに記載の通信方法。

【請求項５０】　前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合に当該高位の認証を行ったことを記録し、

前記認証工程では、前記事業者設備は、前記高位の認証を行ったことが記録されていることをさらなる条件として、前記認証を行う、請求項４２ないし請求項４９のいずれかに記載の通信方法。

【請求項５１】　前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合には、それ以前の通信によって行われた商取引が成立したものとして記録し、前記高位の認証を行わない場合には、それ以前の通信によって行われた前記商取引が成立しなかったものとして記録する、請求項４２ないし請求項５０のいずれかに記載の通信方法。

【請求項５２】　前記認証工程において、前記事業者設備は、前記認証を行う場合には前記通信を継続し、前記認証を行わない場合には前記通信を中止する、請求項３８ないし請求項５１のいずれかに記載の通信方法。

【請求項５３】　通信事業者設備を媒介した無線通信と前記通信事業者設備を媒介しない無線通信網の形成とが可能な端末装置を携帯する群衆が集合ないし通行する空間において、前記群衆の中の少なくとも一部の複数人が携帯する前記端末装置の間で前記無線通信網を形成することにより、前記通信事業者設備を媒介した前記無線通信を行い得ない領域が前記空間の中にあっても、前記空間の中での前記端末装置どうしの通信を可能とした通信方法。

【請求項５４】　前記無線通信網を形成する前記複数の端末装置の一部が、前記通信事業者設備を媒介した前記無線通信を行うことにより、前記無線通信網を形成する前記複数の端末装置の他の一部が、前記無線通信網を媒介しさらに前記通信事業者設備を媒介した通信をも行うことを可能とした、請求項５３に記載の通信方法。

【請求項５５】　前記無線通信網を形成する前記複数の端末装置の少なくとも一部であって、前記無線通信網を媒介して相互に通信する一組の端末装置が、それぞれを識別する符号を相互に交換することにより共通鍵を算出し、当該共通鍵にもとづいて暗号化した形式で通信信号をやりとりする、請求項５３または請求項５４に記載の通信方法。

【請求項５６】　前記無線通信網を媒介した通信を、緊急非常通信に限って可能とした、請求項５３ないし請求項５５のいずれかに記載の通信方法。

【請求項５７】　前記無線通信網の形成が可能な別の端末装置を、前記通信事業者設備を媒介した前記無線通信

10

を行い得ない前記領域に設置し、それにより、前記端末装置を携帯する前記群衆の密度が低い場合でも、前記無線通信網の形成を可能とした、請求項５３ないし請求項５６のいずれかに記載の通信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、半導体装置、端末装置および通信方法に関する。

【０００２】

【従来の技術】携帯電話機等の端末装置の不正使用、すなわち、識別番号を変更するなどにより、自己の端末装置を、通信ネットワークの中で、あたかも他人の端末装置であるかのように見せかけて、料金支払いの義務を逃れるなどの犯罪が、近年において増加していると云われている。この不正使用は、当然ながら他の犯罪と同様に、法律的な処罰を通じて社会的に規制されるべきものであるが、同時に、不正使用を行うことを技術的に困難なものとすること、すなわち不正使用に対する技術的障壁（セキュリティ）を高めることが、犯罪を防止する上で特に重要な対策の一つであると認識されている。

【０００３】図６４は、「日経エレクトロニクス」1999年2月8日号（no. 736），pp. 155-162（以下、文献１）に掲載された記事から引用した説明図であり、携帯電話機に関して現在実施されている不正防止対策の一例を示している。文献１に記載されるように、図６４の方法は、現行の不正防止対策の中で最もセキュリティの高い方法と云われており、「認証」という手順を利用している。

【０００４】この方法では、携帯電話機のシリアル番号（ESN：Electronic Serial Number）、携帯電話機と通信事業者の認証センタとが共有する共有秘密データ（SSD：Shared Secret Data）、および、モバイル識別番号（MIN：Mobile Identification Number）が、携帯電話機ごとに付与される。これらの識別番号は、CAVE（Cellular Authentication and Voice Encryption）アルゴリズムにもとづいて、AUTHREQと称される暗号へと符号化される。暗号化の際に、通信事業者のモバイル交換センタから出力されるRANDと称される乱数が用いられる。

【０００５】通信事業者は、携帯電話機から送信された暗号AUTHREQを、CAVEアルゴリズムにもとづいて復号化する。復号化されて得られた識別番号は、認証センタのみが把握する共有秘密データSSDを含む識別番号と比較され、その結果に応じて、通信の許可または不許可の判定がなされる。このように、携帯電話機と通信事業者との間でのみ共有される共有秘密データSSDにもとづいて、携帯電話機の使用者が正当使用者であるか否かのチェック、すなわち、認証が行われる。

【０００６】

【発明が解決しようとする課題】しかしながら、現行の中で最も強力な不正防止対策であるとされる図６４の認証方式に対しても、この認証をかわして不正使用を行う

という犯罪が、広がりつつあると云われている。その技術上の原因の一つが、文献１にも記載されるように、携帯電話機に付与される識別番号が、書き換え可能なフラッシュメモリ（フラッシュROM）に書き込まれていることにあると云われている。

【０００７】図６５は、携帯電話機の内部構成を簡単に示すブロック図である。従来の携帯電話機９０３には、通信回路９０７とともに、フラッシュメモリ９０８が備わっている。通信回路９０７は、フラッシュメモリ９０８に書き込まれたプログラムにしたがって動作する。識別番号もフラッシュメモリ９０８に保持されており、通信回路９０７は、フラッシュメモリ９０８から読み出された識別番号ＩＤにもとづいて符号化を行い、符号化によって生成された暗号AUTHREQを通信事業者へ送信する。

【０００８】記憶媒体として、書き換え可能なフラッシュメモリ９０８が用いられるのは、通信事業者が行うプログラム変更、例えば、新しい通信方式に対応したプログラムへの変更などに対応する必要があるためである。さらに、書き換え不能なマスクROMが用いられると、プログラム変更に対応できないだけでなく、マスクROMを製造する過程で、個体毎に異なる識別番号に対応した異なるマスクパターンを用いて、識別番号を記録する必要があり、製造効率の低下、および、製造コストの上昇がもたらされるからである。

【０００９】本願出願人によって先になされた出願（特願平11-178173号；以下、文献２）は、多結晶体を有する半導体素子を半導体基板に形成し、多結晶体の結晶構造のばらつきに由来する電気的特性のばらつきを、識別番号の生成に利用することにより、上記した原因を除去する技術を開示している。

【００１０】一方、端末装置の不正使用として、識別番号を書き換えることによって行われる形態だけでなく、端末装置に搭載されている半導体基板（半導体チップ）を不正に取り替えることによって行われる形態も知られている。すなわち、ある識別番号が記録された半導体基板を、別の識別番号が記録された半導体基板に取り替えることにより、自己の端末装置を他人の端末装置であるかのように見せかけて、料金支払いの義務を逃れる等の不正使用の形態も出現している。また、端末装置に限らず、例えば賭博性のある遊技機（我国において「パチンコ台」と通称される遊技機はその代表例）などをも含めた一般の半導体装置の応用機器において、半導体基板を取り替えて不正使用を行うことにより、不法利得を得るという犯罪も知られている。

【００１１】さらに、通信事業者設備を媒介して無線通信を行う携帯可能な端末装置（すなわち携帯電話機）において、端末装置を使用していながら、その紛失を装って、料金支払いの義務を逃れるという不正使用の形態も知られている。

【００１２】この発明は、従来の技術における上記した問題点を解消するためになされたもので、様々な形態での不正使用に対する技術的障壁を高めることのできる半導体装置、端末装置および通信方法を得ることを目的としており、さらに、これらの技術を利用することにより無線通信における利便性を高めた端末装置および通信方法を提供することを目的とする。

【００１３】

【課題を解決するための手段】第１の発明の装置は、半導体装置において、少なくとも一つの半導体基板の各々に形成され、その半導体基板に固有の識別符号を生成する符号生成部と、前記識別符号の各々ごとに、対応する半導体基板とは別の半導体基板に形成され、対応する識別符号に一致する符号を記憶符号として記憶するメモリと、を備える。

【００１４】第２の発明の装置では、第１の発明の半導体装置において、前記メモリが、前記記憶符号を記憶するＯＴＰＲＯＭを備える。

【００１５】第３の発明の装置では、第１または第２の発明の半導体装置において、前記符号生成部が、半導体素子と、前記半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより、前記識別符号を生成し、出力する符号化回路と、を備える。

【００１６】第４の発明の装置では、第３の発明の半導体装置において、前記半導体素子が多結晶体を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する。

【００１７】第５の発明の装置では、第１または第２の発明の半導体装置において、前記符号生成部が、前記識別符号を記憶するＯＴＰＲＯＭを備える。

【００１８】第６の発明の装置は、第１ないし第５のいずれかの発明の半導体装置において、前記識別符号の各々ごとに、前記識別符号と、対応する前記記憶符号とを比較し、これら双方が一致するか否かを判定し、その結果を表現する判定信号を出力する比較回路を、さらに備える。

【００１９】第７の発明の装置では、第６の発明の半導体装置において、前記比較回路が、比較対象とする識別符号に対応する前記半導体基板に形成されている。

【００２０】第８の発明の装置は、第７の発明の半導体装置において、前記識別符号の各々ごとに、対応する前記半導体基板に形成された鍵生成部、暗号化回路および復号化回路を、さらに備え、前記鍵生成部は、対応する前記半導体基板に固有である暗号化のための鍵を生成し、前記暗号化回路は、対応する前記半導体基板に形成された前記符号生成部が生成する前記識別符号を、対応する前記鍵にもとづいて暗号化し、暗号化された形式で対応する前記メモリへ伝え、対応する前記メモリは、前記暗号化回路が出力する暗号化された形式での前記識別

符号を、暗号化された形式での前記記憶符号として記憶し、前記復号化回路は、対応する前記メモリに記憶される暗号化された前記記憶符号を、対応する前記鍵にもとづいて復号化し、前記比較回路は、対応する前記符号化回路が生成する前記識別符号と、対応する前記復号化回路が生成する復号化された前記記憶符号とを比較する。

【００２１】第９の発明の装置では、第８の発明の半導体装置において、前記鍵生成部が、別の半導体素子と、前記別の半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより、前記鍵を生成し、出力する別の符号化回路と、を備える。

【００２２】第１０の発明の装置では、第９の発明の半導体装置において、前記別の半導体素子が多結晶体を有しており、前記別の半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する。

【００２３】第１１の発明の装置では、第８の発明の半導体装置において、前記鍵生成部が、前記鍵を記憶するＯＴＰＲＯＭを備える。

【００２４】第１２の発明の装置は、第７ないし第１１のいずれかの発明の半導体装置において、前記識別符号の各々ごとに、対応する前記半導体基板に形成され、対応する前記符号化回路が生成した前記識別符号の、対応する前記メモリへの送出と、対応する前記メモリに記憶される前記記憶符号の前記比較回路への入力とを、排他的に行うスイッチ回路を、さらに備える。

【００２５】第１３の発明の装置は、第６ないし第１２のいずれかの発明の半導体装置において、前記識別符号の各々に対応した前記判定信号に依存して選択的に動作または非動作となる回路部分を含む所定回路を、さらに備える。

【００２６】第１４の発明の装置では、第１３の発明の半導体装置において、前記所定回路が、前記比較回路が形成されている前記少なくとも一つの半導体基板の一つに形成されている。

【００２７】第１５の発明の装置では、第１ないし第１４のいずれかの発明の半導体装置において、前記少なくとも一つの半導体基板の個数が単一である。

【００２８】第１６の発明の装置では、第１ないし第１４のいずれかにの発明の半導体装置において、前記少なくとも一つの半導体基板の個数が２個であり、前記識別符号の各々ごとに、対応する前記符号生成部と前記メモリは、互いに前記２個の半導体基板の一方と他方とに形成されている。

【００２９】第１７の発明の装置は、端末装置であって、半導体素子と当該半導体素子の電気的特性のばらつきに由来して値がばらつくように前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより暗号化のための鍵を生成し、出力する符号化回路とを備える

鍵生成部と、前記鍵にもとづいて送信データを暗号化する暗号化回路と、前記鍵にもとづいて受信データを復号化する復号化回路と、を備える。

【００３０】第１８の発明の装置では、第１７の発明の端末装置において、前記符号化回路と前記復号化回路とが本体部に組み込まれており、前記鍵生成部が、前記本体部に脱着自在の補助部に組み込まれている。

【００３１】第１９の発明の装置では、第１８の発明の端末装置において、前記補助部がＩＣカードである。

【００３２】第２０の発明の装置では、第１７ないし第１９のいずれかの発明の端末装置において、前記半導体素子が多結晶体を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する。

【００３３】第２１の発明の装置は、端末装置であって、第１３または第１４の発明の半導体装置を備え、前記所定回路が、外部との間で信号を送信および受信する通信回路であって、前記判定信号の各々が前記識別符号の少なくとも一つと対応する前記記憶符号との間の不一致を示すときには、送信または受信の少なくとも一方を停止する。

【００３４】第２２の発明の装置は、端末装置であって、第６ないし第１２のいずれかの発明の半導体装置と、外部との間で信号を送信および受信する通信回路と、を備え、前記通信回路は、前記信号の一部として前記判定信号の各々を前記外部へ送信する。

【００３５】第２３の発明の装置は、端末装置であって、第１ないし第５のいずれかの発明の半導体装置と、外部との間で信号を送信および受信する通信回路と、を備え、前記通信回路は、前記信号の一部として前記識別符号の各々と前記記憶符号の各々とを前記外部へ送信する。

【００３６】第２４の発明の装置では、第２３の発明の端末装置において、前記少なくとも一つの半導体基板の個数が単一であって、前記符号生成部の各々と前記通信回路とが本体部に組み込まれており、前記メモリの各々が前記本体部に脱着自在の補助部に組み込まれている。

【００３７】第２５の発明の装置では、第２４の発明の端末装置において、前記本体部には、暗号化のための第１鍵を生成する第１鍵生成部と、前記符号生成部が生成する前記識別符号を、前記第１鍵にもとづいて暗号化する第１暗号化回路と、がさらに組み込まれており、前記補助部には、暗号化のための第２鍵を生成する第２鍵生成部と、前記メモリが記憶する前記記憶符号を、前記第２鍵にもとづいて暗号化する第２暗号化回路と、がさらに組み込まれており、前記第１暗号化回路は、前記第２暗号化回路が暗号化した前記記憶符号をも、前記第１鍵にもとづいて暗号化し、前記通信回路は、前記第１暗号化回路で暗号化された形式で、前記識別符号および前記記憶符号を前記外部へ送信する。

【００３８】第２６の発明の装置では、第２５の発明の端末装置において、前記第１鍵生成部と前記第１暗号化回路とが、前記符号化回路が形成された前記半導体基板に形成されている。

【００３９】第２７の発明の装置では、第２５または第２６の発明の端末装置において、前記第２鍵生成部と前記第２暗号化回路とが、前記メモリが形成された前記半導体基板に形成されている。

【００４０】第２８の発明の装置では、第２４ないし第２７のいずれかの発明の端末装置において、前記本体部が、充電可能な電池を備えており、前記補助部が、前記本体部に装着されることにより前記電池を充電する充電器である。

【００４１】第２９の発明の装置では、第２４ないし第２７のいずれかの発明の端末装置において、前記補助部がＩＣカードであり、前記本体部と前記補助部の各々には、前記補助部から前記本体部への符号の伝送を無線で媒介するための通信インタフェースが、さらに組み込まれている。

【００４２】第３０の発明の装置では、第２２ないし第２９のいずれかの発明の端末装置において、前記通信回路が、前記少なくとも一つの半導体基板の一つに前記符号生成部とともに形成されている。

【００４３】第３１の発明の装置は、端末装置であって、通信事業者設備を媒介した無線通信を行う通信回路と、前記通信事業者設備を媒介しない無線通信網を形成することにより無線通信を行う無線通信網回路と、を備える。

【００４４】第３２の発明の装置は、第３１の発明の端末装置において、前記通信回路と前記無線通信網回路との間での通信信号の経路の接続と切断とを選択自在に実行することにより、前記無線通信網を通じての前記端末装置の使用者と他者との間の通信と、前記無線通信網を通じての前記端末装置の使用者以外の複数の他者どうしの通信の中継と、を選択自在に実現する切替回路を、さらに備える。

【００４５】第３３の発明の装置は、第３２の発明の端末装置において、暗号化のための鍵を生成する鍵生成部と、前記通信信号の中で前記通信回路から前記無線通信網回路へ送られる送信信号を前記鍵にもとづいて暗号化する暗号化回路と、前記通信信号の中で前記無線通信網回路から前記通信回路へ送られる受信信号を前記鍵にもとづいて復号化する復号化回路と、をさらに備え、前記鍵生成部が、前記端末装置を識別するための符号を生成する符号生成部と、前記符号生成部が生成する前記符号と、前記無線通信網回路を通じて通信相手から送られる別の符号とにもとづいて、前記使用者と前記通信相手との間で共通に使用可能な共通鍵を算出する鍵演算部と、を備える。

【００４６】第３４の発明の装置では、第３３の発明の端末装置において、前記符号生成部が、半導体素子と、前記半導体素子の電気的特性のばらつきに由来して値がばらつくように、前記半導体素子の電気的特性をデジタル形式の信号へ変換することにより、前記符号を生成し、出力する符号化回路と、を備える。

【００４７】第３５の発明の装置では、第３４の発明の端末装置において、前記半導体素子が多結晶体を有しており、前記半導体素子の前記電気的特性のばらつきが、前記多結晶体の結晶構造のばらつきに由来する。

【００４８】第３６の発明の装置では、第３３の発明の端末装置において、前記符号生成部が、前記符号を記憶するＯＴＰＲＯＭを備える。

【００４９】第３７の発明の装置は、第３２ないし第３６のいずれかの発明の端末装置において、前記通信信号の中で前記無線通信網回路から前記通信回路へ送られる受信信号の経路に介挿された第１および第２ミキサを、さらに備え、前記第１ミキサは、前記通信回路が受信した受信信号を復調し、前記第２ミキサは、復調された前記受信信号を前記通信回路の周波数帯域内の周波数を有する搬送波を用いて変調する。

【００５０】第３８の発明の方法は、事業者設備と第２２の発明の端末装置とが相互に通信を行う通信方法であって、(a)前記端末装置が、前記判定信号の各々を前記事業者設備へ送信する工程と、(b)前記事業者設備が、受信した前記判定信号の各々が、前記識別符号の各々と対応する前記記憶符号との一致を示すという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備える。

【００５１】第３９の発明の方法は、事業者設備と第２３の発明の端末装置とが相互に通信を行う通信方法であって、(a)前記端末装置が、前記識別符号の各々と前記記憶符号の各々を前記事業者設備へ送信する工程と、(b)前記事業者設備が、受信した前記識別符号の各々を対応する前記記憶符号と比較し、一致するか否かを判定する工程と、(c)前記事業者設備が、前記工程(b)において前記識別符号の各々が対応する前記記憶符号に一致すると判定したという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備える。

【００５２】第４０の発明の方法は、第３９の発明の通信方法において、(e)前記事業者設備が、受信した前記識別符号の各々と前記記憶符号の各々を記録する工程を、さらに備える。

【００５３】第４１の発明の方法は、第３９の発明の通信方法であって、前記工程(c)において、前記事業者設備は、前記認証を行わない場合には、受信した前記識別符号の各々と前記記憶符号の各々を記録する。

【００５４】第４２の発明の方法は、(a)事業者設備

17

が、第２４の発明の端末装置の前記識別符号を得て、第１登録符号として記憶する工程と、(b)前記事業者設備が、前記端末装置の前記記憶符号を得て、第２登録符号として記憶する工程と、(c)前記工程(a)および(b)の後に、前記事業者設備と前記端末装置とが相互に通信を行う通信工程と、を備え、当該通信工程(c)は、(c-1)前記補助部が前記本体部に装着されていないときに実行される第１通信工程と、(c-2)前記補助部が前記本体部に装着されているときに実行される第２通信工程と、を備え、前記第１通信工程(c-1)は、(c-1-1)前記端末装置が、前記識別符号を前記事業者設備へ送信する工程と、(c-1-2)前記事業者設備が、受信した前記識別符号と前記第１登録符号とを比較し、これら双方が一致するか否かを判定する工程と、(c-1-3)前記事業者設備が、前記工程(c-1-2)で前記双方が一致すると判定したという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備え、前記第２通信工程(c-2)は、(c-2-1)前記端末装置が、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、(c-2-2)前記事業者設備が、受信した前記識別符号と前記第１登録符号とを比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号と前記第２登録符号とを比較し、これら双方が一致するか否かを判定する工程と、(c-2-3)前記事業者設備が、前記工程(c-2-2)の２つの判定のいずれにおいても一致するとの判定が得られたという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの高位の認証を行い、前記条件が充足されなければ、前記高位の認証を行わない高位認証工程と、を備える。

【００５５】第４３の発明の方法は、第４２の発明の通信方法であって、前記工程(b)では、前記補助部が前記本体部に装着された状態で前記事業者設備と前記端末装置とが通信を行うことにより、事業者設備が、前記端末装置の前記記憶符号を得る。

【００５６】第４４の発明の方法では、第４２または第４３の発明の通信方法において、前記工程(c)が、(c-3)前記補助部が前記本体部に装着されているときに実行され、前記第２登録符号の変更を行う変更工程を、さらに備え、前記変更工程(c-3)は、(c-3-1)前記端末装置が、前記変更の意志を表現する要求信号とともに、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、(c-3-2)前記事業者設備が、受信した前記識別符号と前記第１登録符号とを比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号と前記第２登録符号とを比較し、これら双方が一致するか否かを判定する工程と、(c-3-3)前記事業者設備が、前記工程(c-3-2)の２つの判定のいずれにおいても一致するとの判定結果を得たときに限って、前記変更を許可する工程と、(c-3-4)前記工程(c-3-3)の後に、前記端末装置の前記補助部を交換し、交換後の補助部を前記本体部へ装着する工程と、(c-3-5)前記端末装置が、前記工程(c-3-4)の後に、前記識別符号と交換後の前記補助部にもとづく変更後の前記記憶符号とを前記事業者設備へ送信する工程と、(c-3-6)前記事業者設備が、前記工程(c-3-3)で前記変更を許可した場合に限って、受信した変更後の前記記憶符号で前記第２登録符号を更新する工程と、を備える。

18

【００５７】第４５の発明の方法は、(a)事業者設備が、第２５の発明の端末装置の前記識別符号および前記第１鍵を得て、それぞれ第１登録符号および登録鍵として記憶する工程と、(b)前記事業者設備が、前記端末装置の前記第２鍵で暗号化された前記記憶符号を得て、第２登録符号として記憶する工程と、(c)前記工程(a)および(b)の後に、前記事業者設備と前記端末装置とが相互に通信を行う通信工程と、を備え、当該通信工程(c)は、(c-1)前記補助部が前記本体部に装着されていないときに実行される第１通信工程と、(c-2)前記補助部が前記本体部に装着されているときに実行される第２通信工程と、を備え、前記第１通信工程(c-1)は、(c-1-1)前記端末装置が、前記第１暗号化回路で暗号化された形式で、前記識別符号を前記事業者設備へ送信する工程と、(c-1-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第１登録符号と比較し、これら双方が一致するか否かを判定する工程と、(c-1-3)前記事業者設備が、前記工程(c-1-2)で前記双方が一致すると判定したという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの認証を行い、前記条件が充足されなければ、前記認証を行わない認証工程と、を備え、前記第２通信工程(c-2)は、(c-2-1)前記端末装置が、前記第１暗号化回路で暗号化された形式で、前記識別符号および記憶符号を前記事業者設備へ送信する工程と、(c-2-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第１登録符号と比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号を前記登録鍵にもとづいて復号化した上で、前記第２登録符号と比較し、これら双方が一致するか否かを判定する工程と、(c-2-3)前記事業者設備が、前記工程(c-2-2)の２つの判定のいずれにおいても一致するとの判定が得られたという条件が充足されれば、前記端末装置の使用者が正当使用者であるとの高位の認証を行い、前記条件が充足されなければ、前記高位の認証を行わない高位認証工程と、を備える。

【００５８】第４６の発明の方法は、第４５の発明の通信方法であって、前記工程(b)では、前記補助部が前記本体部に装着された状態で前記事業者設備と前記端末装置とが通信を行うことにより、事業者設備が、前記端末装置の前記第２鍵で暗号化された前記記憶符号を得る。

【００５９】第４７の発明の方法では、第４５または第

４６の発明の通信方法において、前記工程(c)が、(c-3)前記補助部が前記本体部に装着されているときに実行され、前記第２登録符号の変更を行う変更工程を、さらに備え、前記変更工程(c-3)は、(c-3-1)前記端末装置が、前記変更の意志を表現する要求信号とともに、前記第１暗号化回路で暗号化された形式で、前記識別符号および前記記憶符号を前記事業者設備へ送信する工程と、(c-3-2)前記事業者設備が、受信した前記識別符号を前記登録鍵にもとづいて復号化した上で、前記第１登録符号と比較し、これら双方が一致するか否かを判定するとともに、受信した前記記憶符号を前記登録鍵にもとづいて復号化した上で、前記第２登録符号と比較し、これら双方が一致するか否かを判定する工程と、(c-3-3)前記事業者設備が、前記工程(c-3-2)の２つの判定のいずれにおいても一致するとの判定結果を得たときに限って、前記変更を許可する工程と、(c-3-4)前記工程(c-3-3)の後に、前記端末装置の前記補助部を交換し、交換後の補助部を前記本体部へ装着する工程と、(c-3-5)前記端末装置が、前記工程(c-3-4)の後に、前記第１暗号化回路で暗号化された形式で、前記識別符号と交換後の前記補助部にもとづく変更後の前記記憶符号とを前記事業者設備へ送信する工程と、(c-3-6)前記事業者設備が、前記工程(c-3-3)で前記変更を許可した場合に限って、受信した変更後の前記記憶符号を前記登録鍵にもとづいて復号化することにより得られる符号で、前記第２登録符号を更新する工程と、を備える。

【００６０】第４８の発明の方法は、第４２ないし第４７のいずれかの発明の通信方法であって、前記高位認証工程において、前記事業者設備は、前記高位の認証を行わない場合には、前記工程(c-2-2)で各登録符号との比較の対象とされた各符号を記録する。

【００６１】第４９の発明の方法は、第４２ないし第４８のいずれかの発明の通信方法であって、前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合には、それ以前の通信に対する通信料金を、裏付けられたものとして記録する。

【００６２】第５０の発明の方法は、第４２ないし第４９のいずれかの発明の通信方法であって、前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合に当該高位の認証を行ったことを記録し、前記認証工程では、前記事業者設備は、前記高位の認証を行ったことが記録されていることをさらなる条件として、前記認証を行う。

【００６３】第５１の発明の方法は、第４２ないし第５０のいずれかの発明の通信方法であって、前記高位認証工程において、前記事業者設備は、前記高位の認証を行う場合には、それ以前の通信によって行われた商取引が成立したものとして記録し、前記高位の認証を行わない場合には、それ以前の通信によって行われた前記商取引が成立しなかったものとして記録する。

【００６４】第５２の発明の方法は、第３８ないし第５１のいずれかの発明の通信方法であって、前記認証工程において、前記事業者設備は、前記認証を行う場合には前記通信を継続し、前記認証を行わない場合には前記通信を中止する。

【００６５】第５３の発明の方法は、通信方法であって、通信事業者設備を媒介した無線通信と前記通信事業者設備を媒介しない無線通信網の形成とが可能な端末装置を携帯する群衆が集合ないし通行する空間において、前記群衆の中の少なくとも一部の複数人が携帯する前記端末装置の間で前記無線通信網を形成することにより、前記通信事業者設備を媒介した前記無線通信を行い得ない領域が前記空間の中にあっても、前記空間の中での前記端末装置どうしの通信を可能とする。

【００６６】第５４の発明の方法は、第５３の発明の通信方法において、前記無線通信網を形成する前記複数の端末装置の一部が、前記通信事業者設備を媒介した前記無線通信を行うことにより、前記無線通信網を形成する前記複数の端末装置の他の一部が、前記無線通信網を媒介しさらに前記通信事業者設備を媒介した通信をも行うことを可能とする。

【００６７】第５５の発明の方法では、第５３または第５４の発明の通信方法において、前記無線通信網を形成する前記複数の端末装置の少なくとも一部であって、前記無線通信網を媒介して相互に通信する一組の端末装置が、それぞれを識別する符号を相互に交換することにより共通鍵を算出し、当該共通鍵にもとづいて暗号化した形式で通信信号をやりとりする。

【００６８】第５６の発明の方法は、第５３ないし第５５のいずれかに記載の通信方法において、前記無線通信網を媒介した通信を、緊急非常通信に限って可能とする。

【００６９】第５７の発明の方法は、第５３ないし第５６のいずれかに記載の通信方法において、前記無線通信網の形成が可能な別の端末装置を、前記通信事業者設備を媒介した前記無線通信を行い得ない前記領域に設置し、それにより、前記端末装置を携帯する前記群衆の密度が低い場合でも、前記無線通信網の形成を可能とする。

【００７０】

【発明の実施の形態】はじめに、本明細書で用いる用語について説明する。本明細書において、符号に関して「一致」とは、完全一致に限定されず、あらかじめ定められた範囲内での近似をも包含する。

【００７１】［1. 実施の形態１］実施の形態１では、２個の半導体基板の一方に固有の識別符号を他方に記憶させておくことにより、半導体基板を取り替えて行われる不正使用を防止する半導体装置、およびその応用機器としての端末装置について説明する。

【００７２】［1.1. 半導体装置］図１は、実施の形態

１による半導体装置の構成を示すブロック図である。この半導体装置６００は、符号生成部４００、比較回路４０３および所定回路４０５、およびメモリ６０１を備えている。符号生成部４００、比較回路４０３および所定回路４０５は、半導体基板ＣＨ１に形成されており、メモリ６０１は別の半導体基板ＣＨ２に形成されている。半導体基板ＣＨ１，ＣＨ２は、モールドされた形態およびベアチップのいずれであってもよく、単一または複数の回路基板の上に搭載されている。

【００７３】符号生成部４００は、半導体基板ＣＨ１に固有の識別符号Ｃｄを生成する。メモリ６０１は、符号生成部４００が生成した識別符号Ｃｄを記憶符号Ｃｏとして記憶する。識別符号Ｃｄは、半導体装置６００が製品として出荷されるときに、符号生成部４００からメモリ６０１へ送信され、メモリ６０１へ書き込まれる。

【００７４】比較回路４０３は、符号生成部４００が生成する識別符号Ｃｄとメモリ６０１から読み出された記憶符号Ｃｏとを比較し、これら双方が互いに一致するか否かを判定し、その結果を表現する判定信号Ｅｎを出力する。一致性の判定として、完全一致性を判定するのであれば、比較回路４０３は、双方の符号の差がゼロであるか否かを判定する従来周知のコンパレータを備えれば足りる。あらかじめ定められた範囲内での近似性を判定するのであれば、比較回路４０３は、双方の符号の差の大きさを、一定の基準値と比較すればよい。差の大きさは、例えば、数値としての差の大きさ、あるいは互いに相違するビット数で評価することが可能である。また、基準値を外部から入力可能とし、半導体装置６００のユーザが所望の値に基準値を設定できるように、半導体装置６００を構成することも可能である。

【００７５】所定回路４０５は、所定の機能を果たすべく複数の回路素子によって形成された回路であり、比較回路４０３が出力する判定信号Ｅｎにもとづいて選択的に動作または非動作となる回路部分を含んでいる。図６５に示した通信回路９０７は、所定回路４０５の一例となり得る。

【００７６】半導体装置６００は以上のように構成されるので、符号生成部４００が生成する識別符号Ｃｄとメモリ６０１から読み出される記憶符号Ｃｏとが互いに一致したときのみ、所定回路４０５のすべての部分が動作する。したがって、所定回路４０５を応用機器の機能を実現する回路の一部とすることにより、比較の結果に応じて、応用機器の所定の動作を許可および不許可することができる。半導体基板ＣＨ１またはＣＨ２を、別の半導体基板に取り替えて応用機器を不正に使用しようとしても、識別符号Ｃｄと記憶符号Ｃｏとが一致しないので、応用機器は所定の動作をなし得ない。半導体装置６００が組み込まれた応用機器は、このようにして半導体基板の取り替えによる不正使用を防止することができる。

【００７７】符号生成部４００と比較回路４０３とが単一の半導体基板ＣＨ３に形成され、所定回路４０５はそれとは別の半導体基板に形成されても良い。しかしながら、所定回路４０５が符号生成部４００および比較回路４０３とともに、単一の半導体基板ＣＨ１に形成される形態では、比較回路４０３から所定回路４０５へ入力される判定信号Ｅｎを、外部から入力することができない。このため、不正使用に対する障壁がさらに高められるという利点が得られる。

【００７８】また、符号生成部４００が形成される半導体基板とは別の半導体基板に比較回路４０３が形成されても良い。しかしながら、比較回路４０３が符号生成部４００とともに単一の半導体基板ＣＨ１またはＣＨ３に形成される形態では、符号生成部４００から比較回路４０３へ入力される識別符号Ｃｄを外部から不正に変更することができない。このため、不正使用に対する障壁が、さらに高められるという利点が得られる。

【００７９】さらに、半導体装置６００が所定回路４０５を備えない形態を実施することも可能である。この場合には、所定回路４０５を、半導体装置６００とは別個に、応用機器に形成すると良い。あるいは、判定信号Ｅｎを応用機器の外部へ取り出し、その値に応じて、外部から応用機器の動作、非動作を指示することができるように、応用機器を構成することも可能である。後述する実施の形態３の端末装置はそのような応用機器の一例である。

【００８０】また、半導体装置６００が所定回路４０５も比較回路４０３も備えない形態を実施することも可能である。この場合には、所定回路４０５および比較回路４０３を、半導体装置６００とは別個に、応用機器に形成すると良い。あるいは、識別符号Ｃｄと記憶符号Ｃｏとを応用機器の外部へ取り出し、その値に応じて、外部から応用機器の動作、非動作を指示することができるように、応用機器を構成することも可能である。後述する実施の形態４の端末装置はそのような応用機器の一例である。

【００８１】［1.2. 符号生成部］図２は、符号生成部４００の内部構成の好ましい一例を示すブロック図である。図２の例では、符号生成部４００は、半導体素子４０１および符号化回路４０２を備えている。符号化回路４０２は、半導体素子４０１の電気的特性をアナログ信号Ａｎとして読み出し、デジタル信号へ変換する。変換によって得られたデジタル信号は、識別符号Ｃｄとして出力される。

【００８２】半導体素子４０１の電気的特性として、半導体素子４０１の個体毎にばらつきを持った特性が選ばれる。それにより、識別符号Ｃｄは、半導体素子４０１の個体毎にばらついた値として生成されるので、符号生成部４００が形成されている半導体基板に固有の識別符号としての性格を備えることとなる。量産される多数の

半導体装置６００の間で、同一工程で製造された半導体素子４０１を用いることができるので、半導体装置６００の製造を簡略化することができる。また、識別符号Ｃｄのもとになる半導体素子４０１の電気的特性を外部から変更することができないので、識別符号Ｃｄの不正な変更に対する障壁が高いという利点も得られる。

【００８３】電気的特性として、半導体装置４０１が多結晶体を備え、その結晶構造のばらつきに由来してばらつく特性を利用することが可能である。この例については、以下の図３～図６で詳述する。また、半導体素子４０１がＭＯＳＦＥＴを備え、その不純物拡散層の不純物濃度のばらつきに起因するしきい値のばらつきを利用することも可能である。

【００８４】図３は、半導体素子４０１の好ましい一例を示す平面図である。図４は、図３のＡ－Ａ切断線に沿った断面図である。この例では、半導体素子４０１は、薄膜トランジスタ（以下、TFTと略記する）１０１を有しており、しかも、そのチャネル領域を含む半導体層１０６０が、多結晶体として形成されている。なお、図３には、説明の便宜のために半導体素子４０１の製造工程の中で中間生成物として形成される半導体層１を描いているが、製造工程の中で選択的エッチングが施されることにより、完成品としての半導体素子４０１では、半導体層１は半導体層１０６０へと成型されている。

【００８５】TFT１０１では、絶縁膜１２の上にゲート電極１１が選択的に形成されており、絶縁膜１２およびゲート電極１１の表面全体が絶縁膜１０で覆われている。絶縁膜１０の上には、半導体層１が形成されている。各要素の材料の一例を述べると、絶縁膜１２はシリコン酸化物であり、ゲート電極１１は不純物がドープされたポリシリコンであり、絶縁膜１０はTEOSなどのシリコン酸化物であり、半導体層１の主成分はシリコンである。

【００８６】半導体層１には、ゲート電極１１の上部に位置するチャネル領域２、ならびに、このチャネル領域２を挟むソース領域３およびドレイン領域４が、形成されている。チャネル領域２に接する絶縁膜１０の部分は、ゲート絶縁膜として機能する。図３および図５の例では、チャネル領域２の導電型は、ｎ型であり、ソース領域３およびドレイン領域４の導電型は、ｐ型である。すなわち、TFT１０１は、一例として、ｐチャネル型のMOS型TFTとして形成されている。いうまでもなく、TFT１０１は、ｎチャネル型のMOS型TFTとして形成されても良い。

【００８７】半導体層１は、多結晶半導体層として形成されており、図３が示すように、無数の結晶粒（グレイン）５、および、それらの境界面に位置し結晶の乱れを生じている部分である結晶粒界（グレインバウンダリ）６を含んでいる。単一の結晶粒５の中では、結晶方位は一様であるが、異なる結晶粒５の間では、結晶方位は一般に異なる。また、結晶粒５の大きさおよび配置はランダムであり、半導体層１を形成する過程で、さまざまにばらつく。すなわち、多数のTFT１０１が同一の製造工程を通じて製造されても、TFT１０１の個体ごとに、半導体層１の結晶構造は異なったものとなる。

【００８８】その結果、図５に例示するように、TFT１０１を仮に一つの個体を表すものとし、これと同一の製造工程で生産された別の個体をTFT１０２として、TFT１０１から仮に区別すると、チャネル領域２を占める結晶粒界６の量は、TFT１０１とTFT１０２の間で同一とはならない。図５は、半導体素子１０１よりもTFT１０２の方が、チャネル領域２に結晶粒界６を少なく含む例を示している。

【００８９】多結晶TFTでは、チャネル領域２に含まれる結晶粒界６の量によって、その特性がばらつくことが知られている。この事実は、例えば、IEEE Transactions onElectron Devices, Vol. 45, No, 1, January (1998), pp. 165-172（以下、文献３）に記載されている。すなわち、図６にTFT１０１および１０２に関して、ゲート電圧Vgとドレイン電流Idとの間の関係を示すように、チャネル領域２に結晶粒界６を多く含むTFT１０１では、結晶粒界６を少なく含むTFT１０２に比べて、同一のゲート電圧Vg0の下でのドレイン電流Idが小さくなる（すなわち、Ida＜Idb）。

【００９０】したがって、TFT１０１が有する多結晶体の結晶構造のばらつきを、半導体基板の識別に利用することが可能となる。個体間で異なる電気的特性は、多結晶体の結晶構造のばらつきに由来するために、フラッシュメモリ９０８（図６５）へ記録された識別番号とは異なり、外部から書き換えることはできない。したがって、応用機器の不正利用に対するセキュリティを高めることができる。

【００９１】しかも、フラッシュメモリ９０８へ識別番号をプログラムする技術とは異なり、プログラムを行う手間を必要としない。さらに、マスクROMに識別番号を記録する技術とは異なり、個体毎に異なる特性が同一の製造工程を通じて得られるので、製造工程が単純であり、製造工数および製造コストが低く抑えられる。さらに、多結晶体の結晶構造のばらつきは大きく、それに由来して電気的特性のばらつきも大きい。このため、識別符号Ｃｄのばらつきの幅を広く確保することが可能である。すなわち、量産される多数の半導体装置６００の間で、互いに識別符号が一致しないようにすることが容易である。

【００９２】なお、製造工程が複雑にはなるが、TFT１０１のチャネル領域２のみが多結晶半導体で形成され、ソース領域３およびドレイン領域４は単結晶半導体で形成されていてもよく、この場合でも同様に、特性はランダムにばらつく。

【００９３】図２～図６に示した半導体素子４０１の電

気的特性は、温度、時間の変化にともなって、微小ながら変化することも有り得る。それにともなって、識別符号Ｃｄは、完全な意味で一定の値を保持するとは限らず、ある程度の変動を伴うことも想定される。これに対処するためには、比較回路４０３は、識別符号Ｃｄの変動をも考慮した許容範囲内で、符号の一致性を判定するとよい。

【００９４】半導体素子４０１が多結晶体を備える例として、図３～図６に示したＴＦＴだけでなく、多結晶体を備える抵抗素子、多結晶体を備える容量素子など、他の素子の例を実施することも可能である。また、半導体素子４０１は、ＴＦＴ等を複数個備えていても良い。ＴＦＴ等の個数が多いほど、識別符号Ｃｄのばらつきの幅が拡大する。これらの例については、実施の形態１２において詳細に説明する。

【００９５】［1.3. ＯＴＰＲＯＭを用いた例］図７は、符号生成部４００の内部構成の好ましい別の一例を示すブロック図である。図７の例では、符号生成部４００は、一回に限り書込が可能な不揮発性メモリであるＯＴＰ(One Time Programable)ＲＯＭ６０２を備えている。半導体装置６００が出荷されるときに、ＯＴＰＲＯＭ６０２には識別符号Ｃｄが書き込まれる。その後、半導体装置６００が使用者の手に渡った後に、ＯＴＰＲＯＭ６０２に書き込まれている識別符号Ｃｄを、書き換えることは技術的に不可能である。すなわち、図７の例においても、符号生成部４００が生成する識別符号Ｃｄの不正な変更に対する技術的障壁が高いという利点が得られる。

【００９６】ＯＴＰＲＯＭは、符号生成部４００だけでなく、図８が示すように、メモリ６０１への利用にも適している。図８の例では、メモリ６０１はＯＴＰＲＯＭ６０２を備えている。半導体装置６００が出荷されるときに、メモリ６０１に備わるＯＴＰＲＯＭ６０２には、符号生成部４００から送信される識別符号Ｃｄが、記憶符号Ｃｏとして書き込まれる。その後、半導体装置６００が使用者の手に渡った後に、ＯＴＰＲＯＭ６０２に書き込まれている記憶符号Ｃｏを、書き換えることは技術的に不可能である。すなわち、図８の例では、メモリ６０１に記憶される記憶符号Ｃｏの不正な変更に対する技術的障壁が高いという利点が得られる。それにより、符号生成部４００が形成された半導体基板を取り替え、それと同時にメモリ６０１に記憶される記憶符号Ｃｏを、新たな半導体基板の識別符号Ｃｄに一致するように書き換えて行われる不正使用をも防止することができる。

【００９７】［1.4. 端末装置］図９は、半導体装置６００の応用機器としての端末装置の構成を示すブロック図である。この端末装置１００１は、携帯電話機として構成されている。端末装置１００１が備える半導体装置１００２は、図１に示した半導体装置６００の一例であり、所定回路４０５として通信回路４０５ａを備えている。

【００９８】好ましくは、符号生成部４００、比較回路４０３および通信回路４０５ａは、単一の半導体基板ＣＨ１００に形成されるが、比較回路４０３および符号生成部４００のみが単一の半導体基板ＣＨ１０２に形成されても良く、符号生成部４００のみが単一の半導体基板に形成されてもよい。いずれの場合であっても、記憶符号Ｃｏを記憶するメモリ６５４は、符号生成部４００が形成される半導体基板とは異なる半導体基板ＣＨ５１に形成される。

【００９９】端末装置１００１の通信を媒介する事業者の設備である通信事業者（必要に応じて、「局」と略記する）設備６５５には、通信回路６５６が備わっている。通信回路４０５ａと通信回路６５６との間で、音声、データなどを内容とする通信信号が、無線（すなわち電波）を媒介としてやり取りされる。端末装置１００１と通信事業者設備６５５とによって、通信システム１０００が構成される。

【０１００】図１０は、通信回路４０５ａの内部構成の一例を示すブロック図である。無線を媒介する端末装置１００１が備える通信回路４０５ａでは、アンテナと信号処理回路（ベースバンド回路）８００の間には、周知の無線周波回路４６２および中間周波回路４６３が介在する。信号処理回路８００には、送信回路４６０と受信回路４６１とが備わっており、通信信号Ｄｔは受信回路４６１によって受信され、送信回路４０６によって送信される。

【０１０１】図１０の例では、送信回路４６０のみが判定信号Ｅｎによってオン・オフする。すなわち、比較回路４０３が符号の不一致を判定すると、送信機能が停止する。受信回路４６１のみ、あるいは送信回路４６０と受信回路４６１の双方が、判定信号Ｅｎにもとづいてオン・オフするように通信回路４０５を構成することも可能である。

【０１０２】図１１は、端末装置１００１が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置６００（より特定的には、半導体装置１００１）が製造される（Ｓ２０１）。その最終工程、ないしそれ以前に、識別符号Ｃｄがメモリ６０１へ記憶符号Ｃｏとして記録される（Ｓ２０２）。その後、半導体装置６００が電話機メーカへ納入され、電話機メーカによって端末装置１００１が組み立てられる（Ｓ２０３）。完成した端末装置１００１は、使用者（ユーザ）へ供給された後（Ｓ２０４）、使用者による通信への利用に供される（Ｓ２０５）。

【０１０３】ステップＳ２０６～Ｓ２１０は、端末装置１００１を用いた通信の手順、すなわちステップＳ２０５の内部フローを表している。通信が開始されると、端末装置１００１は、記憶符号Ｃｏをメモリ６０１から読み出す（Ｓ２０６）。つぎに、比較回路４０３によっ

て、識別符号Ｃｄと記憶符号Ｃｏとの比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号Ｅｎが生成される（Ｓ２０７）。

【０１０４】判定信号Ｅｎが符号の一致を示すときには（Ｓ２０８）、通信回路４０５ａは通信機能を維持することにより、通信処理を続行する（Ｓ２０９）。一方、判定信号Ｅｎが符号の不一致を示すときには（Ｓ２０８）、通信回路４０５ａは送信機能または受信機能の少なくとも一方を停止することにより、通信を不能にする（Ｓ２１０）。通信が完了すると、処理は終了する。

【０１０５】以上のように、端末装置１００１では、判定信号Ｅｎが符号の不一致を示すときには、通信回路４０５ａの少なくとも一部の機能が停止するので、半導体基板を取り替えて通信に使用するという不正行為が、通信事業者設備６５５による処理を待つことなく、端末装置１００１それ自体の働きによって自動的に抑えられる。

【０１０６】なお、以上の説明では、端末装置として無線を通信媒体とする携帯電話機を例としたが、通信ケーブルを通信媒体とする有線の電話機に対しても、本実施の形態は、同様に適用可能である。また、電話機に限らず様々な端末装置に対しても適用可能である。

【０１０７】図１２は、本実施の形態が適用可能な様々な端末装置、および、端末装置が通信の対象とする事業者設備（サーバ）を例示している。例えば、端末装置は、高速道路の使用料金の支払い等を自動的に管理する高速道路管理システムと通信する自動車端末であってもよく、銀行のＡＴＭシステムと通信して現金の引き出し・預金等を行うＩＣカードあるいはパーソナルコンピュータであってもよい。

【０１０８】［2. 実施の形態２］実施の形態２では、実施の形態１の半導体装置および端末装置において、固有の識別符号で識別される半導体基板の個数が単数から複数へ拡張された形態について説明する。

【０１０９】図１３は、実施の形態２による半導体装置の構成を示すブロック図である。図１３が示す半導体装置６２０では、半導体基板ＣＨ４に符号生成部４００、比較回路４０３および所定回路４０５の他に、メモリ６０１が形成されており、別の半導体基板ＣＨ５にはメモリ６０１の他に、符号生成部４００および比較回路４０３が形成されている。半導体基板ＣＨ４に形成された符号生成部４００は、半導体基板ＣＨ４に固有の識別符号Ｃｄ１を生成し、半導体基板ＣＨ５に形成された符号生成部４００は、半導体基板ＣＨ５に固有の識別符号Ｃｄ２を生成する。

【０１１０】半導体基板ＣＨ４に形成されたメモリ６０１は、半導体基板ＣＨ５に形成された符号生成部４００から送信される識別符号Ｃｄ２を記憶符号Ｃｏ２として記憶し、半導体基板ＣＨ５に形成されたメモリ６０１は、半導体基板ＣＨ４に形成された符号生成部４００から送信される識別符号Ｃｄ１を記憶符号Ｃｏ１として記憶する。すなわち、二つの半導体基板ＣＨ４，ＣＨ５のそれぞれに固有の識別符号Ｃｄ，Ｃｄ２が、他方の半導体基板に形成されたメモリ６０１に記憶される。

【０１１１】半導体基板ＣＨ４に形成された比較回路４０３は、識別符号Ｃｄ１と記憶符号Ｃｏ１とを比較し、半導体基板ＣＨ５に形成された比較回路４０３は、識別符号Ｃｄ２と記憶符号Ｃｏ２とを比較する。半導体基板ＣＨ４に形成された所定回路４０５は、二つの比較回路４０３が出力する判定信号Ｅｎ１，Ｅｎ２の組にもとづいて、選択的に動作または非動作となる回路部分を含んでいる。所定回路４０５は、例えば図１０の通信回路４０５ａにおいて、判定信号Ｅｎ１，Ｅｎ２のいずれか一方が符号の不一致を示しているときには、送信回路５６０は動作を停止するように構成することができる。それによって、半導体基板の取り替えによる不正使用に対する障壁をさらに高めることが可能となる。

【０１１２】固有の識別符号Ｃｄが付与される半導体基板の個数を、３個以上に拡張することも可能である。例えば、３個の半導体基板のそれぞれに、固有の識別符号Ｃｄを生成する符号生成部４００とメモリ６０１とが形成され、メモリ６０１は、それ自身が形成されている半導体基板とは別の半導体基板に形成された符号生成部４００から送信される識別符号Ｃｄを記憶するように半導体装置を構成しても良い。あるいは、３個のメモリ６０１の少なくとも一部を、符号生成部４００が形成されている３個の半導体基板とは別の半導体基板に形成しても良い。

【０１１３】識別符号Ｃｄが付与された半導体基板、すなわち符号生成部４００を備える半導体基板の個数が多いほど、応用機器の不正使用に対する障壁を、より高めることができる。また、メモリ６０１を符号生成部４００を備える半導体基板にのみ形成することによって、半導体基板の個数を最小に抑えることができる。特に、図１３に示した半導体装置６２０では、半導体基板の個数を、図１に示した半導体装置６００における半導体基板の個数と同等の２個に抑えつつ、不正使用に対する障壁を高めることができるという利点が得られる。

【０１１４】図１４は、半導体装置６２０の応用機器としての端末装置の構成を示すブロック図である。この端末装置１０１１は、携帯電話機として構成されており、通信事業者設備６５５とともに、通信システム１０１０を構成する。端末装置１０１１が備える半導体装置１０１２は、図１３に示した半導体装置６２０の一例であり、所定回路４０５として通信回路４０５ａを備えている。通信回路４０５ａは、判定信号Ｅｎ１，Ｅｎ２のいずれかが、符号の不一致を示すときには、その一部の機能を停止する。

【０１１５】好ましくは、識別符号Ｃｄ１を生成する符号生成部４００、識別符号Ｃｄ１を比較対象とする比較

回路４０３、記憶符号Ｃｏ２を記憶するメモリ６０１および通信回路４０５ａは、単一の半導体基板ＣＨ１０３に形成されるが、比較回路４０３、メモリ６０１および符号生成部４００のみが単一の半導体基板ＣＨ１１に形成されても良く、符号生成部４００のみが単一の半導体基板ＣＨ１０４に形成されてもよい。また、好ましくは、記憶符号Ｃｏ１を記憶するメモリ６０１は、識別符号Ｃｄ２を生成する符号生成部４００、および識別符号Ｃｄ２を比較の対象とする比較回路４０３とともに、単一の半導体基板ＣＨ１３に形成される。

【０１１６】図１５は、端末装置１０１１が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置６２０（より特定的には、半導体装置１０１２）が製造される（Ｓ２４１）。その最終工程、ないしそれ以前に、各半導体基板の識別符号Ｃｄ１、Ｃｄ２が、他方の半導体基板のメモリ６０１へ記憶符号Ｃｏ１，Ｃｏ２として記録される（Ｓ２４２）。その後、半導体装置６２０が電話機メーカへ納入され、電話機メーカによって端末装置１０１１が組み立てられる（Ｓ２４３）。完成した端末装置１０１１は、使用者へ供給された後（Ｓ２４４）、使用者による通信への利用に供される（Ｓ２４５）。

【０１１７】ステップＳ２４６～Ｓ２５０は、端末装置１０１１を用いた通信の手順、すなわちステップＳ２４５の内部フローを表している。通信が開始されると、端末装置１０１１は、記憶符号Ｃｏ１およびＣｏ２を二つのメモリ６０１から読み出す（Ｓ２４６）。つぎに、一方の比較回路４０３によって、識別符号Ｃｄ１と記憶符号Ｃｏ１との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号Ｅｎ１が出力されると同時に、他方の比較回路４０３によって、識別符号Ｃｄ２と記憶符号Ｃｏ２との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号Ｅｎ２が出力される（Ｓ２４７）。

【０１１８】判定信号Ｅｎ１，Ｅｎ２のいずれもが、符号の一致を示すときには（Ｓ２４８）、通信回路４０５ａは通信機能を維持することにより、通信処理を続行する（Ｓ２４９）。一方、判定信号Ｅｎ１，Ｅｎ２のいずれかが、符号の不一致を示すときには（Ｓ２４８）、通信回路４０５ａは送信機能または受信機能の少なくとも一方を停止することにより、通信を不能にする（Ｓ２５０）。通信が完了すると、処理は終了する。

【０１１９】［3. 実施の形態３］実施の形態３では、実施の形態１または２による半導体装置の中で、所定回路を除いた部分を利用した端末装置について説明する。

【０１２０】図１６は、実施の形態３による端末装置の構成を示すブロック図である。この端末装置１００１は、通信回路４０５ａが比較回路４０３から送られる判定信号Ｅｎにもとづいて動作または非動作を選択的に行うのではなく、判定信号Ｅｎを通信信号の一部として通信事業者設備６５５へ、単に送信する点において、図９に示した実施の形態１の端末装置１００１とは特徴的に異なっている。

【０１２１】図１６の端末装置１００１が通信への利用に供されるまでの処理の流れは、図１１のフローチャートと同等に描かれる。ただし、ステップＳ２０５の内部フローは、図１７のステップＳ１０００の処理へ置き換えられる。ステップＳ１０００の処理が開始されると、端末装置１００１は、記憶符号Ｃｏをメモリ６０１から読み出す（Ｓ２０６）。つぎに、比較回路４０３によって、識別符号Ｃｄと記憶符号Ｃｏとの比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号Ｅｎが生成される（Ｓ２０７）。

【０１２２】この判定信号Ｅｎは、通信回路４０５ａを通じて通信事業者設備６５５へ送信される（Ｓ２０８，Ｓ１００１，Ｓ１００３）。言い換えると、判定信号Ｅｎが符号の一致を示すときには（Ｓ２０８）、判定信号Ｅｎとして符号の一致を示す所定の値が送信され（Ｓ１００１）、判定信号Ｅｎが符号の不一致を示すときには（Ｓ２０８）、上記所定の値は送信されない（Ｓ１００３）。

【０１２３】通信事業者設備６５５は、判定信号Ｅｎが符号の一致を示すときには、端末装置１００１の使用者が正当使用者であるとの認証を行い、判定信号Ｅｎが符号の不一致を示すときには、認証を行わない。通信事業者設備６５５は、例えば、認証を行うときには通信を許可して通信処理を続行し（Ｓ１００２）、認証を行わないときには、通信を不許可として、通信処理を中止する（Ｓ１００４）。

【０１２４】このように、図１６の端末装置１００１では、判定信号Ｅｎを通信事業者設備６５５の側で行われる認証処理の判断材料に供することができ、それにより、半導体基板の取り替えによる不正使用を認証の対象から排除して、精度の高い認証を実現することができる。なお、認証処理にともなう処理として、通信の継続または中止以外に、商取引の許可または不許可など、何らかのサービスの提供または不提供を行うことが可能である。あるいは、単に認証の判断材料を記録しておくという処理を行っても良い。これらの具体例については、後の実施の形態で説明する。

【０１２５】図１８は、実施の形態３による端末装置の別の構成例を示すブロック図である。この端末装置１００１１は、通信回路４０５ａが比較回路４０３から送られる判定信号Ｅｎ１，Ｅｎ２にもとづいて動作または非動作を選択的に行うのではなく、判定信号Ｅｎ１，Ｅｎ２を通信信号の一部として通信事業者設備６５５へ、単に送信する点において、図１４に示した実施の形態１の端末装置１０１１とは特徴的に異なっている。

【０１２６】図１８の端末装置１０１１が通信への利用に供されるまでの処理の流れは、図１５のフローチャー

トと同等に描かれる。ただし、ステップＳ２４５の内部フローは、図１９のステップＳ１０１０の処理へ置き換えられる。ステップＳ１０１０の処理が開始されると、端末装置１０１１は、記憶符号Ｃｏ１，Ｃｏ２を二つのメモリ６０１から読み出す（Ｓ２４６）。つぎに、一方の比較回路４０３によって、識別符号Ｃｄ１と記憶符号Ｃｏ１との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号Ｅｎ１が生成される。それと同時に、他方の比較回路４０３によって、識別符号Ｃｄ２と記憶符号Ｃｏ２との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号Ｅｎ２が生成される。（Ｓ２４７）。

【０１２７】これらの判定信号Ｅｎ１，Ｅｎ２は、通信回路４０５ａを通じて通信事業者設備６５５へ送信される（Ｓ２４８，Ｓ１００１，Ｓ１００３）。言い換えると、判定信号Ｅｎ１，Ｅｎ２のいずれもが、符号の一致を示すときには（Ｓ２４８）、判定信号Ｅｎ１，Ｅｎ２として符号の一致を示す所定の値が送信され（Ｓ１００１）、判定信号Ｅｎ１，Ｅｎ２のいずれかが、符号の不一致を示すときには（Ｓ２０８）、上記所定の値は送信されない（Ｓ１００３）。

【０１２８】通信事業者設備６５５は、判定信号Ｅｎ１，Ｅｎ２のいずれもが、符号の一致を示すときには、端末装置１００１の使用者が正当使用者であるとの認証を行い、判定信号Ｅｎ１，Ｅｎ２のいずれかが符号の不一致を示すときには、認証を行わない。通信事業者設備６５５は、例えば、認証を行うときには通信を許可して通信処理を続行し（Ｓ１００２）、認証を行わないときには、通信を不許可として、通信処理を中止する（Ｓ１００４）。

【０１２９】このように、図１８の端末装置１００１では、判定信号Ｅｎ１，Ｅｎ２を通信事業者設備６５５の側で行われる認証処理の判断材料に供することができ、それにより、半導体基板の取り替えによる不正使用を認証の対象から排除して、精度の高い認証を実現することができる。また、二つの判定信号Ｅｎ１，Ｅｎ２が判断材料とされるので、図１６の端末装置１００１よりもさらに、認証の精度を高めることができる。

【０１３０】［4. 実施の形態４］実施の形態４では、実施の形態１または２による半導体装置の中で、所定回路および比較回路の双方を除いた部分を利用した端末装置について説明する。

【０１３１】図２０は、実施の形態４による端末装置の構成を示すブロック図である。この端末装置８０１が備える半導体装置６５２は、比較回路４０３が除去され、通信回路４０５ａが識別符号Ｃｄおよび記憶符号Ｃｏを通信信号の一部として通信事業者設備６５５へ、単に送信する点において、図９に示した実施の形態１の半導体装置１００２とは特徴的に異なっている。

【０１３２】図２０の通信事業者設備６５５は、通信回路６５６に加えて、判定回路６５７および顧客データメモリ６５８を備えている。通信事業者設備６５５と端末装置８０１とは、通信システム８００を構成している。

【０１３３】端末装置８０１が通信への利用に供されるまでの処理の流れは、図１１のフローチャートと同等に描かれる。ただし、ただし、ステップＳ２０５の内部フローは、図２１のステップＳ２６０の処理へ置き換えられる。ステップＳ２６０の処理が開始されると、端末装置８０１は、識別符号Ｃｄおよび記憶符号Ｃｏを通信事業者設備６５５へ送信する（Ｓ２６１）。それにともない、通信事業者設備６５５は、通信回路６５６によって識別符号Ｃｄおよび記憶符号Ｃｏを受信する（Ｓ２６２）。

【０１３４】つぎに、通信事業者設備６５５は、判定回路６５７によって、識別符号Ｃｄと記憶符号Ｃｏとを比較し、双方が互いに一致するか否かを判定し、判定結果を示す判定信号Ｅｎを通信回路６５６へ伝える（Ｓ２６３）。通信事業者設備６５５は、判定信号Ｅｎが符号の一致を示すときには（Ｓ２６４）、端末装置８０１の使用者が正当使用者であるとの認証を行い、判定信号Ｅｎが符号の不一致を示すときには（Ｓ２６４）、認証を行わない。通信事業者設備６５５は、例えば、認証を行うときには通信を許可して通信処理を続行し（Ｓ２６５）、認証を行わないときには、通信を不許可として、通信処理を中止する（Ｓ２６８）。

【０１３５】また、識別符号Ｃｄおよび記憶符号Ｃｏを記録するよう指示がなされている場合には（Ｓ２６６）、認証を行わない場合に識別符号Ｃｄおよび記憶符号Ｃｏが顧客データメモリ６５８へ記録される（Ｓ２６７）。そして、例えば通信処理が中止された（Ｓ２７８）後に、識別符号Ｃｄおよび記憶符号Ｃｏを、過去に記録された顧客データメモリ６５８の内容と照合することにより（Ｓ２６９）、不正使用者の特定がなされる（Ｓ２７０）。

【０１３６】認証を行わないときに、通信処理を中止することなく、識別符号Ｃｄおよび記憶符号Ｃｏの記録（Ｓ２６７）のみを行うことも可能である。さらに、識別符号Ｃｄおよび記憶符号Ｃｏの記録（Ｓ２６７）を、認証結果とは無関係に実行することも可能である。後者の場合には、ステップＳ２６７の処理は、例えば、ステップＳ２６３とＳ２６４の間で実行される。

【０１３７】このように、図２０の端末装置８０１では、識別符号Ｃｄおよび記憶符号Ｃｏを通信事業者設備６５５の側で行われる認証処理の判断材料に供することができ、それにより、半導体基板の取り替えによる不正使用を認証の対象から排除して、精度の高い認証を実現することができる。

【０１３８】図２２は、実施の形態４による端末装置の別の構成例を示すブロック図である。この端末装置８１１が備える半導体装置６５２は、比較回路４０３が除去

され、通信回路４０５ａが識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２を通信信号の一部として通信事業者設備６５５へ、単に送信する点において、図１４に示した実施の形態１の半導体装置１０１２とは特徴的に異なっている。

【０１３９】図２２の通信事業者設備６５５は、通信回路６５６に加えて、判定回路６５７および顧客データメモリ６５８を備えている。通信事業者設備６５５と端末装置８１１とは、通信システム８１０を構成している。

【０１４０】端末装置８１１が通信への利用に供されるまでの処理の流れは、図１５のフローチャートと同等に描かれる。ただし、ただし、ステップＳ２４５の内部フローは、図２３のステップＳ２８０の処理へ置き換えられる。ステップＳ２８０の処理が開始されると、端末装置８１１は、識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２を通信事業者設備６５５へ送信する（Ｓ２１１）。それにともない、通信事業者設備６５５は、通信回路６５６によって識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２を受信する（Ｓ２７２）。

【０１４１】つぎに、通信事業者設備６５５は、判定回路６５７によって、識別符号Ｃｄ１と記憶符号Ｃｏ１とを比較し、双方が互いに一致するか否かを判定するとともに、識別符号Ｃｄ２と記憶符号Ｃｏ２とを比較し、双方が互いに一致するか否かを判定する。そして、それらの判定結果を示す判定信号Ｅｎを通信回路６５６へ伝える（Ｓ２７３）。通信事業者設備６５５は、二つの比較の双方において符号の一致が認められたときには（Ｓ２７４）、端末装置８１１の使用者が正当使用者であるとの認証を行い、二つの比較のいずれかにおいて符号の不一致が認められたときには（Ｓ２７４）、認証を行わない。通信事業者設備６５５は、例えば、認証を行うときには通信を許可して通信処理を続行し（Ｓ２７５）、認証を行わないときには、通信を不許可として、通信処理を中止する（Ｓ２７８）。

【０１４２】また、識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２を記録するよう指示がなされている場合には（Ｓ２７６）、認証を行わない場合に識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２が顧客データメモリ６５８へ記録される（Ｓ２７７）。そして、例えば通信処理が中止された（Ｓ２７８）後に、識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２を、過去に記録された顧客データメモリ６５８の内容と照合することにより（Ｓ２７９）、不正使用者の特定がなされる（Ｓ２８０）。

【０１４３】認証を行わないときに、通信処理を中止することなく、識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２の記録（Ｓ２７７）のみを行うことも可能である。さらに、識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２の記録（Ｓ２７７）を、認証結果とは無関係に実行することも可能である。後者の場合には、

ステップＳ２７７の処理は、例えば、ステップＳ２７３とＳ２７４の間で実行される。

【０１４４】このように、図２３の端末装置８１１では、識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２を通信事業者設備６５５の側で行われる認証処理の判断材料に供することができ、それにより、半導体基板の取り替えによる不正使用を認証の対象から排除して、精度の高い認証を実現することができる。また、二つの識別符号Ｃｄ１，Ｃｄ２が比較の対象とされるので、図２１の端末装置８０１よりもさらに、認証の精度を高めることができる。

【０１４５】［5. 実施の形態５］実施の形態５では、実施の形態１または２による半導体装置において、半導体基板の間での識別符号Ｃｄおよび記憶符号Ｃｏのやりとりを、暗号化した形式で行う形態について説明する。

【０１４６】図２４は、実施の形態５による半導体装置の構成を示すブロック図である。図２４が示す半導体装置６３０では、符号生成部４００が形成されている半導体基板ＣＨ２０またはＣＨ２２に、暗号化回路６３１、復号化回路６３２および鍵生成部６３３が形成されている。

【０１４７】鍵生成部６３３は暗号化のための鍵Ｋを生成する。鍵Ｋは、識別符号Ｃｄと同様に、半導体基板ＣＨ２０またはＣＨ２２に固有の符号として生成される。暗号化回路６３１は、符号生成部４００が生成する識別符号Ｃｄを、鍵生成部６３３が生成する鍵Ｋにもとづいて識別符号Ｃｄ＃へと暗号化し、半導体基板ＣＨ２１に形成されたメモリ６０１へ送出する。メモリ６０１は、暗号化された識別符号Ｃｄ＃を、暗号化された記憶符号Ｃｏ＃として記憶する。

【０１４８】復号化回路６３２は、メモリ６０１に記憶されている暗号化された記憶符号Ｃｏ＃を読み出し、鍵生成部６３３が生成する鍵Ｋにもとづいて記憶符号Ｃｏへと復号化し、比較回路４０３へ供給する。所定回路４０５は、比較回路４０３が出力する判定信号Ｅｎにもとづいて、動作または非動作となる回路部分を含んでいる。

【０１４９】以上のように、半導体装置６３０では、異なる半導体基板の間で、暗号化された形式で識別符号Ｃｄおよび記憶符号Ｃｏがやりとりされるので、識別符号Ｃｄおよび記憶符号Ｃｏのいずれをも外部から読み取ることができない。このため、不正使用に対する障壁がさらに高められる。

【０１５０】図２５は、鍵生成部６３３の内部構成の一例を示すブロック図である。図２５の例では、鍵生成部６３３は、ＯＴＰＲＯＭ６０２を備えており、鍵Ｋは、半導体装置６３０の出荷時にＯＴＰＲＯＭ６０２に書き込まれる。このため、鍵生成部６３３が生成する鍵Ｋを不正に変更することができない。また、鍵Ｋが半導体装置６３０の出荷時にすでに書き込まれているので、鍵Ｋ

が使用者へ漏洩することがない。

【０１５１】図２６は、鍵生成部６３３の内部構成の別の一例を示すブロック図である。図２６の鍵生成部６３３は、図２に示した半導体素子４０１と符号化回路４０２とを備えている。符号化回路４０２は、半導体素子４０１の電気的特性をアナログ信号Ａｎとして読み出し、デジタル信号へ変換する。変換によって得られたデジタル信号は、鍵Ｋとして出力される。

【０１５２】半導体素子４０１の電気的特性として、半導体素子４０１の個体毎にばらつきを持った特性が選ばれる。それにより、鍵Ｋは、半導体素子４０１の個体毎にばらついた値として生成されるので、鍵生成部６３３が形成されている半導体基板に固有の識別符号としての性格を備えることとなる。鍵Ｋを書き込む必要もなく、さらに、量産される多数の半導体装置６３０の間で、同一工程で製造された半導体素子４０１を用いることができるので、半導体装置６３０の製造を簡略化することができる。また、鍵Ｋのもとになる半導体素子４０１の電気的特性を外部から変更することができないので、鍵Ｋの不正な変更に対する障壁が高いという利点も得られる。

【０１５３】図３～図６に例示したように、半導体装置４０１が多結晶体を備え、その結晶構造のばらつきに由来してばらつく電気的特性を利用することが可能である。多結晶体の結晶構造のばらつきは大きく、それに由来して電気的特性のばらつきも大きいので、鍵Ｋのばらつきの幅を広く確保することが可能である。すなわち、量産される多数の半導体装置６３０の間で、互いに鍵Ｋが一致しないようにすることが容易である。

【０１５４】図２７は、図９の端末装置１００１において、半導体装置１００２の代わりに図２４の半導体装置６３０を用い、所定回路４０５を通信回路４０５ａとした場合に、端末装置１００１が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置６３０が製造される（Ｓ３０１）。その最終工程、ないしそれ以前に、暗号化された識別符号Ｃｄ＃がメモリ６０１へ記憶符号Ｃｏ＃として記録される（Ｓ３０２）。その後、半導体装置６３０が電話機メーカへ納入され、電話機メーカによって端末装置１００１が組み立てられる（Ｓ３０３）。完成した端末装置１００１は、使用者へ供給された後（Ｓ３０４）、使用者による通信への利用に供される（Ｓ３０５）。

【０１５５】ステップＳ３０６～Ｓ３１０は、端末装置１００１を用いた通信の手順、すなわちステップＳ３０５の内部フローを表している。通信が開始されると、端末装置１００１は、記憶符号Ｃｏ＃をメモリ６０１から読み出す（Ｓ３０６）。つぎに、復号化回路６３２によって記憶符号Ｃｏ＃が記憶符号Ｃｏへと復号化されることにより、比較回路４０３によって、識別符号Ｃｄと記憶符号Ｃｏとの比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号Ｅｎが生成される（Ｓ３０７）。

【０１５６】判定信号Ｅｎが符号の一致を示すときには（Ｓ３０８）、通信回路４０５ａは通信機能を維持することにより、通信処理を続行する（Ｓ３０９）。一方、判定信号Ｅｎが符号の不一致を示すときには（Ｓ３０８）、通信回路４０５ａは送信機能または受信機能の少なくとも一方を停止することにより、通信を不能にする（Ｓ３１０）。通信が完了すると、処理は終了する。

【０１５７】図２８は、実施の形態５による半導体装置の別の構成例を示すブロック図である。図２８が示す半導体装置６３５は、図１３の半導体装置６２０において、識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２が、二つの半導体基板の間で、暗号化した形式でやりとりされるように構成されている。すなわち、符号生成部４００、比較回路４０３およびメモリ６０１が形成されている二つの半導体基板ＣＨ２０（またはＣＨ２２）およびＣＨ３の双方に、暗号化回路６３１、復号化回路６３２および鍵生成部６３３が形成されている。

【０１５８】半導体基板ＣＨ２０（またはＣＨ２２）では、鍵生成部６３３は半導体基板ＣＨ２０（またはＣＨ２２）に固有の鍵Ｋ１を生成し、暗号化回路６３１は識別符号Ｃｄ１を鍵Ｋ１にもとづいて識別符号Ｃｄ１＃へと暗号化し、半導体基板ＣＨ２３のメモリ６０１へ送出する。半導体基板ＣＨ２３のメモリ６０１は、識別符号Ｃｄ１＃を記憶符号Ｃｏ１＃として記憶する。半導体基板ＣＨ２０（またはＣＨ２２）の復号化回路６３２は、メモリ６０１から記憶符号Ｃｏ１＃を読み出し、鍵Ｋ１にもとづいて記憶符号Ｃｏ１へと復号化して比較回路４０３へ供給する。

【０１５９】半導体基板ＣＨ２３では、鍵生成部６３３は半導体基板ＣＨ２３に固有の鍵Ｋ２を生成し、暗号化回路６３１は識別符号Ｃｄ２を鍵Ｋ２にもとづいて識別符号Ｃｄ２＃へと暗号化し、半導体基板ＣＨ２０（またはＣＨ２２）のメモリ６０１へ送出する。半導体基板ＣＨ２０（またはＣＨ２２）のメモリ６０１は、識別符号Ｃｄ２＃を記憶符号Ｃｏ２＃として記憶する。半導体基板ＣＨ２３の復号化回路６３２は、メモリ６０１から記憶符号Ｃｏ２＃を読み出し、鍵Ｋ２にもとづいて記憶符号Ｃｏ２へと復号化して比較回路４０３へ供給する。所定回路４０５は、二つの比較回路４０３が出力する二つの判定信号Ｅｎ１，Ｅｎ２の組にもとづいて、動作または非動作となる回路部分を含んでいる。

【０１６０】以上のように、半導体装置６３５では、異なる半導体基板の間で、暗号化された形式で識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２がやりとりされるので、識別符号Ｃｄ１，Ｃｄ２および記憶符号Ｃｏ１，Ｃｏ２のいずれをも外部から読み取ることができない。このため、不正使用に対する障壁がさらに高めら

れる。また、実施の形態２の半導体装置６２０（図１３）と同様に、二つの判定信号Ｅｎ１，Ｅｎ２が用いられるので、半導体基板の取り替えによる不正使用に対する障壁をさらに高めることが可能となる。

【０１６１】また、符号生成部４００が形成された半導体基板が３個以上である半導体装置においても、同様に、暗号化回路６３１、復号化回路６３２および鍵生成部６３３を、各半導体基板に配置することによって、異なる半導体基板の間で識別符号および記憶符号を暗号化した形式でやりとりすることが可能である。

【０１６２】図２９は、図１４の端末装置１０１１において、半導体装置１０１２の代わりに図２８の半導体装置６３５を用い、所定回路４０５を通信回路４０５ａとした場合に、端末装置１０１１が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置６３５が製造される（Ｓ３４１）。その最終工程、ないしそれ以前に、各半導体基板の暗号化された識別符号Ｃｄ１＃、Ｃｄ２＃が、他方の半導体基板のメモリ６０１へ記憶符号Ｃｏ１＃，Ｃｏ２＃として記録される（Ｓ３４２）。その後、半導体装置６２０が電話機メーカへ納入され、電話機メーカによって端末装置１０１１が組み立てられる（Ｓ３４３）。完成した端末装置１０１１は、使用者へ供給された後（Ｓ３４４）、使用者による通信への利用に供される（Ｓ３４５）。

【０１６３】ステップＳ３４６～Ｓ３５０は、端末装置１０１１を用いた通信の手順、すなわちステップＳ３４５の内部フローを表している。通信が開始されると、端末装置１０１１は、記憶符号Ｃｏ１＃およびＣｏ２＃を二つのメモリ６０１から読み出す（Ｓ３４６）。つぎに、二つの復号化回路６３２によって記憶符号Ｃｏ１＃，Ｃｏ２＃が記憶符号Ｃｏ１，Ｃｏ２へと復号化された後、一方の比較回路４０３によって、識別符号Ｃｄ１と記憶符号Ｃｏ１との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号Ｅｎ１が出力されると同時に、他方の比較回路４０３によって、識別符号Ｃｄ２と記憶符号Ｃｏ２との比較が行われ、双方が一致するか否かに関する判定結果を表現する判定信号Ｅｎ２が出力される（Ｓ３４７）。

【０１６４】判定信号Ｅｎ１，Ｅｎ２のいずれもが、符号の一致を示すときには（Ｓ３４８）、通信回路４０５ａは通信機能を維持することにより、通信処理を続行する（Ｓ３４９）。一方、判定信号Ｅｎ１，Ｅｎ２のいずれかが、符号の不一致を示すときには（Ｓ３４８）、通信回路４０５ａは送信機能または受信機能の少なくとも一方を停止することにより、通信を不能にする（Ｓ３５０）。通信が完了すると、処理は終了する。

【０１６５】［6. 実施の形態６］実施の形態６では、実施の形態５による半導体装置において、暗号化された識別符号の送出と、暗号化された記憶符号の入力とを、排他的に行うスイッチ回路が設けられる形態について説明する。

【０１６６】図３０は、実施の形態６による半導体装置の構成を示すブロック図である。図３０が示す半導体装置６４０では、符号生成部４００が形成されている半導体基板ＣＨ４０またはＣＨ４２に、暗号化回路６３１、復号化回路６３２および鍵生成部６３３に加えて、スイッチ回路６４１が形成されている。スイッチ回路６４１は、暗号化回路６３１から半導体基板ＣＨ４１に形成されたメモリ６０１へ送出される識別符号Ｃｄ＃の伝達経路、およびメモリ６０１から復号化回路６３２へ送られる記憶符号Ｃｏ＃の伝達経路に介挿されており、識別符号Ｃｄ＃の伝達と記憶符号Ｃｏ＃の伝達とを排他的に行う。

【０１６７】使用者が不正使用を意図して、暗号化回路６３１が出力する識別符号Ｃｄ＃が復号化回路６３２へそのまま入力されるように、半導体基板ＣＨ４０（またはＣＨ４２）の端子を短絡したとしても、スイッチ回路６４１の働きにより、識別符号Ｃｄ＃が復号化回路６３２へそのまま入力されることはない。すなわち、端子の短絡によって不正使用が意図されても、識別符号Ｃｄと記憶符号Ｃｏとが一致しているかのように比較回路４０３に見せかけることはできない。このように、半導体装置６４０は、半導体基板の端子を短絡することによってなされる応用機器の不正使用をも防止する。

【０１６８】スイッチ回路６４１は、符号生成部４００と暗号化回路６３１との間、および比較回路４０３と復号化回路６３２との間に介挿しても、図３０の半導体装置６４０と同等の効果が得られる。一般に、スイッチ回路６４１は、符号生成部４００からメモリ６０１へ至る識別符号Ｃｄ（またはＣｄ＃）の伝達経路、および、メモリ６０１から比較回路４０３へ至る記憶符号Ｃｏ（またはＣｏ＃）の伝達経路に介挿されておればよい。

【０１６９】また、スイッチ回路６４１は、暗号化回路６３１等を備えない図１の半導体装置６００にも適用可能である。すなわち、図１の半導体装置６００において、符号生成部４００からメモリ６０１へ至る識別符号Ｃｄの伝達経路、およびメモリ６０１から比較回路４０３へ至る記憶符号Ｃｏの伝達経路に介挿されるように、半導体基板ＣＨ１（またはＣＨ３）にスイッチ回路６４１を形成することも可能である。それにより、図３０の半導体装置６４０と同等の効果が得られる。

【０１７０】さらに、スイッチ回路６４１は、図１３に示した半導体装置６２０、および図２８に示した半導体装置６３５に適用することも可能である。図１３の半導体装置６２０に適用される場合には、スイッチ回路６４１は、半導体基板ＣＨ４（またはＣＨ６）と半導体基板ＣＨ５の双方に形成される。図２８の半導体装置６３５に適用される場合には、スイッチ回路６４１は、半導体基板ＣＨ２０（またはＣＨ２２）と半導体基板ＣＨ２３

の双方に形成される。

【０１７１】［7. 実施の形態７］実施の形態５で説明した半導体素子４０１を備える鍵生成部６３３は、ホストコンピュータとデータのやり取りを行う一般の端末装置にも応用可能である。実施の形態７では、そのように構成された端末装置について説明する。

【０１７２】図３１は、実施の形態７による端末装置の構成を示すブロック図である。端末装置８２１とこれに接続されるホストコンピュータ８２５とは、互いにデータＤｄをやり取りするシステム８２０を構成している。端末装置８２１は、データＤｄを入力するデータ入力部８２２、およびデータＤｄを出力するデータ出力部８２３に加えて、暗号化回路６３１、復号化回路６３２および鍵生成部６３３を備えている。鍵生成部６３３は暗号化のための鍵Ｋを生成する。暗号化回路６３１は、データ入力部８２２から入力されたデータＤｄを、鍵生成部６３３が生成する鍵Ｋにもとづいてデータ Ｄｄ＃へと暗号化し、ホストコンピュータ８２５へ送出する。

【０１７３】ホストコンピュータ８２５は、暗号化されたデータＤｄ＃をデータＤｏ＃としてメモリ８２６へ記憶する。復号化回路６３２は、メモリ８２６に記憶されている暗号化されたデータＤｏ＃を受信すると、鍵生成部６３３が生成する鍵ＫにもとづいてデータＤｏへと復号化し、データ出力部８２３へ伝える。データＤｏはデータＤｄと同一である。このように、端末装置８２１では、ホストコンピュータ８２５との間で、暗号化した形式でデータがやりとりされるので、データが表現する情報の漏洩に対する障壁が高い。

【０１７４】鍵生成部６３３の内部構成は、図２６で示される。すなわち、鍵生成部６３３は、半導体素子４０１の個体毎にばらつく電気的特性を利用して、端末装置に固有の鍵Ｋを生成する。したがって、端末装置８２１の製造工程で、鍵Ｋを書き込む必要もなく、さらに、量産される多数の端末装置８２１の間で、同一工程で製造された半導体素子４０１を用いることができるので、端末装置８２１の製造を簡略化することができる。また、鍵Ｋのもとになる半導体素子４０１の電気的特性を外部から変更することができないので、鍵Ｋの不正な変更に対する障壁が高いという利点も得られる。

【０１７５】図３２は、実施の形態７による端末装置の別の構成例を示すブロック図である。図３２の端末装置は、本体部８２８に脱着自在のＩＣカード８２９に鍵生成部６３３が組み込まれている点において、図３１の端末装置８２１とは特徴的に異なっている。ＩＣカード８２９が本体部８２８に装着されることにより、本体部８２８に設けられた暗号化回路６３１および復号化回路６３２が、鍵生成部６３３に接続される。

【０１７６】本体部８２８に脱着自在のＩＣカード８２９に鍵生成部６３３が組み込まれているので、携帯に便利なＩＣカード８２９を自在に持ち運ぶことにより、離れた場所に設置された複数の本体部８２１に対して、同一の鍵Ｋを使用することが可能である。

【０１７７】［8. 実施の形態８］実施の形態８では、実施の形態４による端末装置８０１において、記憶符号Ｃｏを記憶するメモリ６５４が、本体部に脱着自在の補助部に組み込まれている形態について説明する。

【０１７８】図３３は、実施の形態８による端末装置の構成を示すブロック図である。この端末装置は、本体部６５１と、補助部としての充電器６５３とに分離されており、図２０の端末装置８０１において、半導体基板ＣＨ５０を本体部６５１へ組み込み、半導体基板ＣＨ５１を充電器６５３へ組み込んだ装置と同等である。本体部６５１には図示しない充電可能な電池が備わっており、充電器６５３は、本体部６５１へ装着されたときに電池を充電する。

【０１７９】充電器６５３が本体部６５１へ装着されたときには、電池が充電されるだけでなく、半導体基板ＣＨ５０を有する半導体装置６５２と半導体基板ＣＨ５１との間が接続される。通信回路４０５ａは、充電器６５３が本体部６５１へ装着されないときには、識別符号Ｃｄと記憶符号Ｃｏの中で、識別符号Ｃｄのみを通信事業者設備６５５へ送信し、充電器６５３が本体部６５１へ装着されているときには、識別符号Ｃｄと記憶符号Ｃｏの双方を送信する。通信事業者設備６５５、端末装置本体部６５１および充電器６５３は、通信システム６５０を構成する。

【０１８０】図３４は、図３３の端末装置が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置６５２が製造され（Ｓ５０１）、その後、半導体装置６５２が電話機メーカへ納入され、電話機メーカによって端末装置本体部６５１が組み立てられる（Ｓ５０２）。これと並行ないし前後して、部品としてのメモリ６５４が製造され（Ｓ５０３）、その後、電話機メーカによって充電器６５３が組み立てられる（Ｓ５０４）。

【０１８１】端末装置本体部６５１と充電器６５３の双方が完成すると、識別符号Ｃｄが記憶符号Ｃｏとしてメモリ６５４へ記録され（Ｓ５０５）、端末装置本体部６５１と充電器６５３のセットが、通信事業者設備６５５を保有する通信事業者へ納入される（Ｓ５０６）。ステップＳ５０１～Ｓ５０６までのいずれかの段階で、識別符号Ｃｄと記憶符号Ｃｏの双方が読み取られ、通信事業者設備６５５の顧客データメモリ６５８へ登録される（Ｓ５０７）。その後、端末装置本体部６５１および充電器６５３のセットが、使用者へ供給された後（Ｓ５０８）、使用者による通信への利用に供される（Ｓ５０９）。

【０１８２】図３５および図３６は、ステップＳ５０９の内部手順を示すフローチャートである。通信が開始されると、端末装置の使用が非充電時の使用である場合、

すなわち充電器６５３が本体部６５１に装着されていない場合には（Ｓ５２０）、端末装置本体部６５１は、識別符号Ｃｄを通信事業者設備６５５へ送信する（Ｓ５２１）。それにともない、通信事業者設備６５５は、通信回路６５６によって識別符号Ｃｄを受信する（Ｓ５２２）。

【０１８３】つぎに、通信事業者設備６５５は、判定回路６５７によって、識別符号Ｃｄと登録された識別符号Ｃｄとを比較し、双方が互いに一致するか否かを判定し、判定結果を示す判定信号Ｅｎを通信回路６５６へ伝える（Ｓ５２３）。通信事業者設備６５５は、判定信号Ｅｎが符号の一致を示すときには（Ｓ５２４）、端末装置本体部６５１の使用者が正当使用者であるとの認証を行い、判定信号Ｅｎが符号の不一致を示すときには（Ｓ５２４）、認証を行わない。通信事業者設備６５５は、例えば、認証を行うときには通信を許可して通信処理を続行し（Ｓ５２５）、認証を行わないときには、通信を不許可として、通信処理を中止する（Ｓ５２６）。

【０１８４】端末装置の使用が充電時の使用である場合、すなわち本体部６５１が充電器６５３に接続された状態で通信に使用されている場合には（Ｓ５２０，Ｓ５３０）、端末装置本体部６５１は、識別符号Ｃｄと記憶符号Ｃｏの双方を通信事業者設備６５５へ送信する（Ｓ５３１）。それにともない、通信事業者設備６５５は、通信回路６５６によって識別符号Ｃｄおよび記憶符号Ｃｏを受信する（Ｓ５３２）。

【０１８５】つぎに、通信事業者設備６５５は、判定回路６５７によって、識別符号Ｃｄと登録された識別符号Ｃｄとを比較し、双方が互いに一致するか否かを判定するとともに、記憶符号Ｃｏと登録された記憶符号Ｃｏとを比較し、双方が互いに一致するか否かを判定する。判定回路６５７は、二つの判定結果を表現する判定信号Ｅｎを通信回路６５６へ伝える（Ｓ５３３）。

【０１８６】通信事業者設備６５５は、判定信号Ｅｎにもとづいて、いずれの判定においても符号の一致が認められるときには（Ｓ５３４）、端末装置の使用者が正当使用者であるとの認証を行い、いずれかの判定において符号の不一致が認められるときには（Ｓ５３４）、認証を行わない。ステップＳ５３３では、二つの符号Ｃｄ，Ｃｏの双方にもとづいて判定がなされるので、符号Ｃｄのみにもとづいてステップ５２３での判定に比べて、判定の確度が高い。すなわち、ステップＳ５３３の判定にもとづいてなされる認証は、ステップＳ５２３の判定にもとづいてなされる認証に比べて、端末装置が正当に使用されていることをより高い確度で証明する高位の（高レベルの）認証に相当する。

【０１８７】したがって、通信事業者設備６５５は、レベルの異なる二つの認証を、手続の重要性に応じて使い分けることが可能となる。一例として、通信事業者設備６５５は、ステップＳ５３３の判定にもとづいて認証を

行うときには、端末装置が通信に使用されているときに（Ｓ５３５）通信を許可して通信処理を続行する（Ｓ５３６）だけでなく、通信に使用されているか否かに関わりなく、それ以前の通信（前回にステップＳ５３３の判定にもとづいて認証されてから今回までの通信）に対する通信料金を、裏付けられたものとして記録する（Ｓ５３７）。これにより、端末装置の紛失を装って料金支払いの義務を逃れる違法行為を防止することが可能となる。端末装置本体部６５１と充電器６５３との双方を同時に紛失するというケースは希少であるため、裏付けは十分に高い確度を持ったものとなる。

【０１８８】また、通信事業者設備６５５は、ステップＳ５３３の判定にもとづいて認証を行わないときには、すでに登録されている識別符号Ｃｄおよび記憶符号Ｃｏとは別個に、ステップＳ５３２で受信した識別符号Ｃｄおよび記憶符号Ｃｏを、顧客データメモリ６５８へ記録する。記録された識別符号Ｃｄおよび記憶符号Ｃｏは、不正使用者の特定に役立てることができる。

【０１８９】図３４に戻って、ステップＳ５０７では、識別符号Ｃｄと記憶符号Ｃｏの双方が登録される代わりに、識別符号Ｃｄのみが登録されても良い。この場合には、ステップＳ５０１～Ｓ５０６までのいずれかの段階で、識別符号Ｃｄのみが読み取られれば足りる。記憶符号Ｃｏの登録は、使用者がはじめて行う充電時の使用（Ｓ５３０）の際に、ステップＳ５３１で送信される記憶符号Ｃｏを、顧客データメモリ６５８へ登録することにより達成される。

【０１９０】なお、メモリ６０１は、充電器６５３だけでなく、本体部に脱着自在の何らかの補助部に組み込まれても良い。ただし、補助部が充電器６５３である図３３の形態では、使用者に特別の手間を要求することなく、本体部６５１と補助部との結合が定期的に行われるという利点が得られる。

【０１９１】［9. 実施の形態９］実施の形態９では、実施の形態８による端末装置において、本体部と補助部の間、および本体部と通信事業者設備の間において、暗号化された形式で符号が伝送される形態について説明する。

【０１９２】図３７は、実施の形態９による端末装置の構成を示すブロック図である。この端末装置は、本体部６７１が備える半導体装置６７２に、暗号化回路６３１および鍵生成部６３３が設けられており、充電器６５３にも暗号化回路６３１および鍵生成部６７６が設けられている点において、図３３の端末装置とは特徴的に異なる。それにともない、通信事業者設備６７５には、復号化回路６３２が設けられている。通信事業者設備６７５、端末装置本体部６７１および充電器６７３は、通信システム６７０を構成する。

【０１９３】充電器６７３では、鍵生成部６７６は暗号化のための鍵Ｋ２を生成し、暗号化回路６３１はメモリ

６０１から読み出した記憶符号Ｃｏを鍵Ｋ２にもとづいて暗号化し、記憶符号Ｃｏ＃として本体部６７１へ送出する。本体部６７１では、鍵生成部６３３は暗号化のための鍵Ｋ１を生成し、暗号化回路６３１は符号生成部４００が生成する識別符号Ｃｄを鍵Ｋ１にもとづいて暗号化し、識別符号Ｃｄ＃として通信回路４０５ａへ伝える。本体部６７１の暗号化回路６３１は、充電器６７３から送られる記憶符号Ｃｏ＃をも、鍵Ｋ１にもとづいて暗号化し、記憶符号Ｃｏ＃＃として通信回路４０５ａへ伝える。記憶符号Ｃｏ＃＃は、二つの鍵Ｋ１，Ｋ２によって二重に暗号化されている。

【０１９４】通信回路４０５ａは、暗号化された識別符号Ｃｄ＃および記憶符号Ｃｏ＃＃を、通信事業者設備６５５へ送信する。通信事業者設備６５５は、復号化回路６３２によって識別符号Ｃｄ＃および記憶符号Ｃｏ＃＃を、それぞれ識別符号Ｃｄおよび記憶符号Ｃｏ＃へと復号化し、判定回路６５７での判定の材料に供する。

【０１９５】このように、図３７の端末装置では、本体部６７１と充電器６７３の間、および本体部６７１と通信事業者設備６７５の間において、暗号化された形式で符号が伝送されるので、これらの符号の漏洩に対する障壁が高いという利点が得られる。

【０１９６】本体部６７１において、好ましくは、鍵生成部６３３と暗号化回路６３１とは符号生成部４００とともに、単一の半導体基板ＣＨ５０（またはＣＨ７０）に形成される。それによって、鍵Ｋ１および識別符号Ｃｄの漏洩に対する障壁がさらに高められる。同様に、充電器６７３において、鍵生成部６７６と暗号化回路６３１とは、メモリ６０１とともに、単一の半導体基板ＣＨ７１に形成される。それによって、鍵Ｋ２および記憶符号Ｃｏの漏洩に対する障壁がさらに高められる。

【０１９７】図３８は、図３７の端末装置が通信への利用に供されるまでの処理の流れを示すフローチャートである。はじめに、部品としての半導体装置６７２が製造され（Ｓ７０１）、その後、半導体装置６７２が電話機メーカへ納入され、電話機メーカによって端末装置本体部６７１が組み立てられる（Ｓ７０２）。これと並行ないし前後して、部品としてのメモリ６５４が製造され（Ｓ７０３）、その後、電話機メーカによって充電器６７３が組み立てられる（Ｓ７０４）。

【０１９８】端末装置本体部６７１と充電器６７３の双方が完成すると、識別符号Ｃｄが記憶符号Ｃｏとしてメモリ６５４へ記録され（Ｓ７０５）、端末装置本体部６７１と充電器６７３のセットが、通信事業者設備６７５を保有する通信事業者へ納入される（Ｓ７０６）。ステップＳ７０１～Ｓ７０６までのいずれかの段階で、識別符号Ｃｄ、記憶符号Ｃｏ＃および鍵Ｋ１が読み取られ、通信事業者設備６７５の顧客データメモリ６５８へ登録される（Ｓ７０７）。その後、端末装置本体部６７１および充電器６７３のセットが、使用者へ供給された後

（Ｓ７０８）、使用者による通信への利用に供される（Ｓ７０９）。

【０１９９】図３９および図４０は、ステップＳ７０９の内部手順を示すフローチャートである。通信が開始されると、端末装置の使用が非充電時の使用である場合、すなわち充電器６７３が本体部６７１に装着されていない場合には（Ｓ７２０）、端末装置本体部６７１は、識別符号Ｃｄ＃を通信事業者設備６７５へ送信する（Ｓ７２１）。それにともない、通信事業者設備６７５は、通信回路６５６によって識別符号Ｃｄ＃を受信する（Ｓ７２２）。

【０２００】つぎに、通信事業者設備６７５は、復号化回路６３２によって、識別符号Ｃｄ＃を識別符号Ｃｄへと復号化した後、判定回路６５７によって、識別符号Ｃｄと登録された識別符号Ｃｄとを比較し、双方が互いに一致するか否かを判定する。そして、判定回路６５７は、判定結果を示す判定信号Ｅｎを通信回路６５６へ伝える（Ｓ７２３）。通信事業者設備６７５は、判定信号Ｅｎが符号の一致を示すときには（Ｓ７２４）、端末装置本体部６７１の使用者が正当使用者であるとの認証を行い、判定信号Ｅｎが符号の不一致を示すときには（Ｓ７２４）、認証を行わない。通信事業者設備６７５は、例えば、認証を行うときには通信を許可して通信処理を続行し（Ｓ７２５）、認証を行わないときには、通信を不許可として、通信処理を中止する（Ｓ７２６）。

【０２０１】端末装置の使用が充電時の使用である場合、すなわち本体部６７１が充電器６７３に接続された状態で通信に使用されている場合には（Ｓ７２０，Ｓ７３０）、端末装置本体部６７１は、識別符号Ｃｄ＃と記憶符号Ｃｏ＃＃の双方を通信事業者設備６７５へ送信する（Ｓ７３１）。それにともない、通信事業者設備６７５は、通信回路６５６によって識別符号Ｃｄ＃および記憶符号Ｃｏ＃＃を受信する（Ｓ７３２）。

【０２０２】つぎに、通信事業者設備６７５は、復号化回路６３２によって、識別符号Ｃｄ＃を識別符号Ｃｄへと復号化するとともに、記憶符号Ｃｏ＃＃を記憶符号Ｃｏ＃へと復号化する。その後、通信事業者設備６７５は、判定回路６５７によって、識別符号Ｃｄと登録された識別符号Ｃｄとを比較し、双方が互いに一致するか否かを判定するとともに、記憶符号Ｃｏ＃と登録された記憶符号Ｃｏ＃とを比較し、双方が互いに一致するか否かを判定する。判定回路６５７は、二つの判定結果を表現する判定信号Ｅｎを通信回路６５６へ伝える（Ｓ７３３）。

【０２０３】通信事業者設備６７５は、判定信号Ｅｎにもとづいて、いずれの判定においても符号の一致が認められるときには（Ｓ７３４）、端末装置の使用者が正当使用者であるとの認証を行い、いずれかの判定において符号の不一致が認められるときには（Ｓ７３４）、認証を行わない。ステップＳ７３３の判定にもとづいてなさ

れる認証は、ステップＳ７２３の判定にもとづいてなされる認証に比べて、端末装置が正当に使用されていることをより高い確度で証明する高位の（高レベルの）認証に相当する。

【０２０４】一例として、通信事業者設備６７５は、ステップＳ７３３の判定にもとづいて高位の認証を行うときには、端末装置が通信に使用されているときに（Ｓ７３５）通信を許可して通信処理を続行する（Ｓ７３６）だけでなく、通信に使用されているか否かに関わりなく、それ以前の通信（前回にステップＳ７３３の判定にもとづいて認証されてから今回までの通信）に対する通信料金を、裏付けられたものとして記録する（Ｓ７３７）。また、通信事業者設備６７５は、ステップＳ７３３の判定にもとづいて高位の認証を行わないときには、すでに登録されている識別符号Ｃｄおよび記憶符号Ｃｏとは別個に、ステップＳ７３２で受信した識別符号Ｃｄおよび記憶符号Ｃｏを、顧客データメモリ６５８へ記録する。

【０２０５】図３８に戻って、ステップＳ７０７では、識別符号Ｃｄ、記憶符号Ｃｏ＃および鍵Ｋ１が登録される代わりに、識別符号Ｃｄと鍵Ｋ１のみが登録されても良い。この場合には、ステップＳ７０１～Ｓ７０６までのいずれかの段階で、識別符号Ｃｄのみが読み取られれば足りる。記憶符号Ｃｏ＃の登録は、使用者がはじめて行う充電時の使用（Ｓ７３０）の際に、ステップＳ７３１で送信される記憶符号Ｃｏ＃を、顧客データメモリ６５８へ登録することにより達成される。

【０２０６】以上のように、図３７の端末装置を用いることにより、図３３の端末装置を用いた場合と同様に、通信事業者設備６７５は、確度の異なる２段階の認証を、手続の重要性に応じて使い分けることができる。しかも、暗号化された形式で、識別符号Ｃｄおよび記憶符号Ｃｏが送信されるので、これらの符号の漏洩に対する障壁が高い。

【０２０７】充電器６７３を紛失したり、あるいは故障を生じるなどにより、充電器６７３を交換することが必要な場合が想定される。このような場合に、すでに登録されている記憶符号Ｃｏ＃を、あらたな充電器６７３に固有の記憶符号Ｃｏ＃へと更新することができれば、正当使用者にとって都合がよい。それには、図４１が示すように、図４０の処理手順にステップＳ７４１およびＳ７４２を付加するとよい。図４１の処理手順では、記憶符号Ｃｏ＃の変更を行わないときには（Ｓ７４１）、図４１と同様にステップＳ７３１～Ｓ７３８の処理が行われ、記憶符号Ｃｏ＃の変更を行わうときには（Ｓ７４１）、登録された記憶符号Ｃｏ＃を変更する処理が実行される（Ｓ７４２）。

【０２０８】図４２および図４３は、変更処理（Ｓ７４２）の内部手順を示すフローチャートである。変更処理が開始されると、端末装置から通信事業者設備６７５

へ、識別符号Ｃｄ＃、記憶符号Ｃｏ＃＃、および端末識別番号とともに、登録された記憶符号Ｃｏ＃の変更の意志を表現する要求信号が送信される（Ｓ７５２）。それにともない、通信事業者設備６７５は、これらの符号、端末識別番号および信号を通信回路６５６によって受信する（Ｓ７５３）。

【０２０９】つぎに、通信事業者設備６７５は、復号化回路６３２によって、識別符号Ｃｄ＃を識別符号Ｃｄへと復号化するとともに、記憶符号Ｃｏ＃＃を記憶符号Ｃｏ＃へと復号化する。その後、通信事業者設備６７５は、判定回路６５７によって、識別符号Ｃｄと登録された識別符号Ｃｄとを比較し、双方が互いに一致するか否かを判定するとともに、記憶符号Ｃｏ＃と登録された記憶符号Ｃｏ＃とを比較し、双方が互いに一致するか否かを判定する。判定回路６５７は、二つの判定結果を表現する判定信号Ｅｎを通信回路６５６へ伝える（Ｓ７５３）。

【０２１０】通信事業者設備６７５は、判定信号Ｅｎにもとづいて、いずれの判定においても符号の一致が認められるときには（Ｓ７５４）、登録された記憶符号Ｃｏ＃の変更を許可する旨の通知を端末装置へ送信するとともに、新しい記憶符号Ｃｏ＃を持つ充電器６７３への交換を促すメッセージを、端末装置へ送信し表示させる。それに応じて、端末装置の使用者が、記憶符号Ｃｏ＃を有する充電器６７３を、新たな記憶符号Ｃｏ＃（便宜上、ＣｏNew＃と記載する）を有する充電器６７３へと交換すると（Ｓ７５７）、端末装置から通信事業者設備６７５へ、識別符号Ｃｄ＃および記憶符号ＣｏNew＃＃が送信される（Ｓ７５８）。それにともない、通信事業者設備６７５は、これらの識別符号Ｃｄ＃および記憶符号ＣｏNew＃＃を通信回路６５６によって受信する（Ｓ７５３）。

【０２１１】つぎに、通信事業者設備６７５は、復号化回路６３２によって、識別符号Ｃｄ＃を識別符号Ｃｄへと復号化するとともに、記憶符号ＣｏNew＃＃を記憶符号ＣｏMew＃へと復号化する（Ｓ７６０）。その後、通信事業者設備６７５は、顧客データメモリ６５８へ登録されている記憶符号Ｃｏ＃を、記憶符号ＣｏNew＃で更新する。

【０２１２】通信事業者設備６７５は、判定信号Ｅｎにもとづいて、いずれかの判定において符号の不一致が認められるときには（Ｓ７５４）、変更処理をそれ以上進めることなく、現在使用中の充電器６７３をそのまま使用して再度の操作を行うよう促すメッセージを、端末装置へ送信し表示させる（Ｓ７５５）。

【０２１３】ステップＳ７４２と同様の変更処理は、図４０の処理手順だけでなく、暗号を用いない図３６の処理手順にも、付加することが可能である。それにより、使用者は、図３３の充電器６５３を交換することが可能となる。

【０２１４】充電器６５３，６７３が備えるメモリ６５４にＯＴＰＲＯＭを用いる代わりに、書き換え可能なメモリ、例えばフラッシュＲＯＭを用いてもよい。上記した変更処理Ｓ７４２は、このような記憶符号Ｃｏ＃の書き換えが可能な充電器６５３，６７３の使用にも適している。不正な変更に対するセキュリティを高めるために、登録された記憶符号Ｃｏ＃の書き換えを、クレジットカード番号など課金を保証できる情報を端末装置が送信した場合に限定することも可能である。

【０２１５】図４４および図４５は、図３８の通信処理（Ｓ７０９）の別の内部フローを示すフローチャートである。この通信処理（Ｓ７７０）では、認証が商取引へ利用される。すなわち、通信事業者設備６７５は、ステップＳ７３３の判定にもとづいて高位の認証を行うときには（Ｓ７３４）、端末装置が通信に使用されているときに（Ｓ７３５）、通信処理を継続して商取引を許可する（Ｓ７３６）とともに、端末装置が通信に使用されているか否かに関わりなく、それ以前の通信（前回にステップＳ７３３の判定にもとづいて認証されてから今回までの通信）においてなされた商取引が成立したものとして記録する（Ｓ７７５）。一方、通信事業者設備６７５は、ステップＳ７３３の判定にもとづいて高位の認証を行わないときには、それ以前の通信においてなされた商取引が成立しなかったものとして記録する（Ｓ７７６）。

【０２１６】確度の高い認証にもとづいて商取引が成立した旨の記録がなされておれば、取引相手は当該記録にもとづいて、商取引は有効なものとして商品の発送等の様々な手続を進めることが可能であり、商取引が成立しなかった旨の記録が有れば、商取引にもとづく手続を中止することができる。これにより、端末装置の不正使用にもとづく不正な商取引による損害を解消ないし低減することができる。

【０２１７】さらに望ましくは、通信事業者設備６７５は、ステップＳ７３３の判定にもとづいて高位の認証を行わないときには、非充電時の商取引をも不可とするための記録を行う（Ｓ７７７）。記録は、例えば、通信事業者設備６７５が備えるコンピュータシステムのレジスタに、フラグを立てることによって行われる。

【０２１８】端末装置の使用が非充電時の使用である場合、すなわち充電器６７３が本体部６７１に装着されていない場合に（Ｓ７２０）、ステップＳ７２３の判定にもとづいて認証をおこなうときには、非充電時の商取引を不可とする記録がなされているか否か（例えば、上記したフラグが立っているか否か）が判定される（Ｓ７７１）。そして、通信事業者設備６７５は、上記した記録がなされていなければ、通信処理を継続して商取引を許可し（Ｓ７７２）、記録がなされておれば、通信処理を中止する（Ｓ７７３）。

【０２１９】このように、充電器６７３が本体部６７１に装着されない状態でなされる通常の認証に、過去になされた確度の高い判定結果が反映されるので、商取引などの重要な手続を、通常の認証の下で行うことができる。なお、図３５および図３６に示したステップＳ５０９においても、図４４および図４５に示したステップＳ７７２～Ｓ７７３、Ｓ７７４～Ｓ７７７を実行することが可能である。

【０２２０】図３７の充電器６７３は、携帯に便利なＩＣカードに置き換えることも可能である。この場合には、使用者がＩＣカードを時折、本体部６７１へ装着する必要があるが、ＩＣカードから本体部６７１への記憶符号Ｃｏ＃の伝送を、無線を媒体として行うことが可能であれば、使用者が意識的にＩＣカードを本体部６７１へ装着する手間を省くことができ、使用者に便利である。図４６はそのように構成された端末装置を例示するブロック図である。

【０２２１】図４６の端末装置は、本体部６９１が備える半導体装置６９２に、通信インタフェース６９４が設けられており、ＩＣカード６９３にも通信インタフェース６９５が設けられている。通信インタフェース６９４は、例えば、鍵生成部６３３、暗号化回路６３１および符号生成部４００とともに、単一の半導体基板ＣＨ９０（またはＣＨ９１）に形成される。同様に、通信インタフェース６９５は、例えば、鍵生成部６７６、暗号化回路６３１およびメモリ６０１とともに、単一の半導体基板ＣＨ９２に形成される。

【０２２２】通信インタフェース６９４，６９５は、無線通信を行うインタフェースであり、例えば、Bluetooth規格に準拠している。したがって、ＩＣカード６９３から本体部６９１への記憶符号Ｃｏ＃の伝送は、無線を媒介して行われる。このため、例えば、ＩＣカード６９３が使用者の着衣のポケットの中に投入されており、本体部６９１が使用者が携帯する鞄の中に収納されていても、通信事業者設備６７５へ、識別符号Ｃｄ＃と記憶符号Ｃｏ＃＃の双方を送信することが可能となる。ＩＣカード６９３の代わりに、携帯電話機としての本体部に差し込んで使用されるＵＩＭ（Universal subscriber Identification Module）のようなカードを用いてもよい。ただし、その場合には、使用者が本体部とカードとを同時に紛失する可能性が無視できないので、図４６が示すように、別個の独立した機器との間で記憶符号Ｃｏ＃をやり取りする形態がより望ましい。

【０２２３】なお、通信システム６７０において、図１２が示すように、通信事業者設備６５５は、銀行のＡＴＭシステムなど、他の事業者設備に置き換えが可能である。例えば、認証にもとづいて商取引を行う場合には、認証および商取引の許可、不許可等の処理を、端末装置の取引相手である銀行のＡＴＭシステムが直接に行うことも可能である。他の実施の形態における通信システムにおいても同様である。

49

【０２２４】［10. 実施の形態１０］従来においては、地下街あるいはビルディングの中など、電波が侵入し難い領域では、端末装置は通信事業者設備を媒介した無線通信を行い得ないという問題点があった。あるいは、そのような領域において無線通信を可能にするためには、多くの基地局を設ける必要があった。実施の形態１０では、通信事業者設備を媒介した無線通信を行い得ない領域においても、基地局なしで無線通信を可能にする端末装置および通信方法について説明する。本実施の形態による端末装置および通信方法においては、実施の形態５などで示した暗号化回路、復号化回路および鍵生成部が有用な役割を果たす。

【０２２５】［10.1. 概略］図４７は、本実施の形態による通信方法を示す説明図である。この方法では、通信事業者設備を媒介した無線通信と、通信事業者設備を媒介しない無線通信網の形成が可能な端末装置が用いられる。以下に説明する例では、上記無線通信網として、無線ＬＡＮが採用される。電波が侵入し難い領域においても、通常時には群衆が集合ないし通行している。現在においては、これらの群衆の少なからぬ部分が携帯電話機を携帯している。これら群衆が携帯する携帯電話機が、上記した機能を有する端末装置であれば、図４７が示すように、複数の端末装置８４０ａ～８４０ｄの間で無線ＬＡＮを形成することにより、互いに通信を行うことが可能となる。例えば、端末装置８４０ａと端末装置８４０ｄとが、端末装置８４０ｂ，８４０ｃを中継することにより、互いに通信を行うことが可能となる。

【０２２６】無線ＬＡＮとして、例えばBluetooth規格に準拠したものを用いることができる。この場合には、一つの端末装置は、自身を中心とする半径１０ｍ以内にある他の端末装置と、無線を媒介して通信を行うことが可能である。地下街、あるいはビルディングの中には、通常時には１０ｍ以内に多数の通行者、作業者等が存在しており、これらの人々が携帯する端末装置を経由することによって、地下街、あるいはビルディング内の全体をカバーする通信が可能となる。

【０２２７】無線ＬＡＮを利用することにより、小さい電力で運営できるという利点も得られる。例えば１０ｍを到達範囲とする無線ＬＡＮでは、１ｋｍを到達範囲とする無線通信に比べて、電波を発射するのに要する消費電力は（１／１００）^{2}倍である。１ｋｍ離れた端末装置の間で通信を行うために、平均１ｍ間隔で並んだ１０００個の端末装置が通信を中継したとしても、全消費電力は、（１／１００）^{2}×１０００＝１／１０倍に低減される。

【０２２８】また、地下街、あるいはビルディング内のような電波が侵入し難い領域だけでなく、一般に多数の人々が集合、通行ないし居住する空間の中で、無線ＬＡＮを形成することにより、上記空間の全体で端末装置どうしを媒介した通信が実現する。当該空間の中に地下

50

街、あるいはビルディング内のような電波が侵入し難い領域があっても、端末装置どうしを媒介した通信が阻害されることがない。また、各家庭内の端末装置が無線ＬＡＮを中継することにより、地上の住宅街においても、ほとんど基地局のいらない低消費電力の無線通信システムを構築することができる。

【０２２９】［10.2. 端末装置の例］図４７が示す無線ＬＡＮを媒介した通信では、不特定多数の人が携帯する端末装置を経由して通信が行われるために、通信内容の漏洩に対するセキュリティを確保する必要がある。それには図４８が示すように、通信事業者設備を媒介した無線通信を行う部分（遠距離通信部と仮称する）８４７と、無線ＬＡＮを媒介した通信を行う部分（近距離通信部と仮称する）８４８とが、電気的に分離されるように端末装置４８０を構成するとよい。

【０２３０】遠距離通信部８４７は、通信事業者設備を媒介した無線通信を行う通信回路８４１、音声を入力するためのマイク８４２、音声を出力するためのスピーカ８４３、ダイヤル番号などをキー操作等により入力するための入力部８４５、および文字、記号、図形等により情報を表示する表示パネル８４４を備えている。近距離通信部８４８は、無線ＬＡＮを形成することにより無線通信を行う無線ＬＡＮ回路８４６を備えている。図４８の端末装置８４０では、遠距離通信部８４７と近距離通信部８４８とが、互いに分離されているので、端末装置８４０を所持する使用者自身は、無線ＬＡＮを媒介した通信を行うことはできず、単に他人の通信を中継する役割を担うに過ぎない。

【０２３１】端末装置の所持者自身が無線ＬＡＮを媒介した通信を行うことを可能にし、しかも通信内容の漏洩に対するセキュリティを確保するには、図４９が示すように、暗号技術を用いるとよい。通信事業者設備を媒介とした無線通信で暗号技術が用いられる場合であっても、それとは異なる独自の暗号体系が、無線ＬＡＮを媒介とした通信に用いられる。

【０２３２】無線ＬＡＮ回路８４６と通信回路８４１の間には、通信信号の伝達経路が設けられており、この伝達経路には、切替回路８５６、暗号化回路８５１および復号化回路８５２が介挿されている。切替回路８５６は、上記伝達経路の接続と切断とを選択自在に実行する。切替回路８５６が上記伝達経路を接続するときには、端末装置８５０の使用者と他者との間で、無線ＬＡＮを媒介した通信が実現する。切替回路８５６が上記伝達経路を切断するときには、端末装置８５０は無線ＬＡＮを媒介した他者どうしの通信を単に中継するに過ぎない。なお、図４９では、便宜上、アンテナが送信用と受信用とに分けて描かれるが、これらは通常においては単一のアンテナに共通化されている。

【０２３３】暗号化回路８５１、復号化回路８５２および鍵生成部８５３は、端末装置８５０の使用者と他者と

の間で無線ＬＡＮを媒介した通信を行うために、切替回路８５６が上記伝達経路を接続するときに、その機能を果たす。鍵生成部８５３は、暗号化のための鍵Ｋを生成する。暗号化回路８５１は、通信回路８４１から無線ＬＡＮ回路８４６の送信回路８５５へ送られる送信信号を、鍵Ｋにもとづいて暗号化する。復号化回路８５２は、無線ＬＡＮ回路８４６の受信回路８５４から通信回路８４１へ送られる受信信号を鍵Ｋにもとづいて復号化する。

【０２３４】ここで、鍵Ｋは無線ＬＡＮを媒介して端末装置８５０が通信を行う通信相手と共通の鍵である必要がある。そのために、鍵生成部８５３は図５０が示す内部構成を有する。すなわち、鍵生成部８５３は、符号生成部６３３および鍵演算部８５７を備えている。符号生成部６３３は、端末装置８５０に固有な識別符号Ｃｄを生成する。鍵演算部８５７は、無線ＬＡＮ回路８４６を通じて通信相手から送られる別の符号とにもとづいて、端末装置８５０の使用者と通信相手との間で共通に使用可能な共通鍵を算出し、鍵Ｋとして出力する。

【０２３５】符号生成部６３３は、実施の形態５の図２５または図２６に示す形態を採ることが望ましい。それにより、実施の形態５と同様の効果が得られる。図５０は、符号生成部６３３が図２６と同等に形成された例を示している。

【０２３６】［10.3. 鍵生成の手順］図５１は、鍵生成部８５３が鍵Ｋを生成する手順の一例を示すフローチャートである。図５１の手順は、周知のＤＨ法を利用している。端末装置８５０と他の端末装置との間で、無線ＬＡＮを媒介した通信が開始されると、他の端末装置すなわち通信相手が新規であるか否かが判定される（Ｓ８０１）。通信相手が新規であれば、あらかじめ定められた素数ｐと、あらかじめ定められた自然数ｇとにもとづいて、鍵演算部８５７によって、符号$\alpha\#=g^{\alpha}\bmod(p)$が算出される（Ｓ８０２）。ここで、$\alpha$は符号生成部６３３が生成する識別符号Ｃｄである。また、ｍｏｄ（）は、整数論におけるモードを表す。素数ｐおよび自然数ｇは、すべての端末装置の間で共通であり、公開鍵に相当する。

【０２３７】つぎに、算出された符号$\alpha\#$が、通信回路８４１および送信回路８５５を通じて、通信相手へ送信される（Ｓ８０３）。つづいて、通信相手が送信した符号$\beta\#=g^{\beta}\bmod(p)$が、受信回路８５４によって受信され、通信回路８４１を通じて、鍵演算部８５７へ送られる（Ｓ８０４）。つぎに、鍵演算部８５７は、鍵$K=g^{\alpha\beta}\bmod(p)$を算出する（Ｓ８０５）。その後、鍵演算部８５７は、算出した鍵Ｋを、通信相手の識別番号（例えば、電話番号）とともに、メモリ８５８へ記録する（Ｓ８０６）。

【０２３８】つぎに、鍵演算部８５７は、鍵Ｋを暗号化回路８５１および復号化回路８５２へ供給することにより、鍵Ｋを共通鍵とする暗号通信を実現する（Ｓ８０８）。ステップＳ８０８の処理は、通信が終了するまで継続される（Ｓ８０９）。ステップＳ８０１において、通信相手が新規でないと判定されれば、鍵演算部８５７は、鍵Ｋを算出することなく、メモリ８５８へ記録されている鍵Ｋを読み出し（Ｓ８０７）、ステップＳ８０８，Ｓ８０９の処理を実行する。ステップＳ８０１の判定は、メモリ８５８に記録が存在するか否かにもとづいて行うことができる。

【０２３９】以上のように、通信相手と識別符号を交換することにより生成された共通鍵にもとづいて暗号通信が行われるので、通信内容の漏洩を防止しつつ、任意の通信相手との通信を実現することができる。なお、図５１に手順において、ステップＳ８０１およびＳ８０７を除去して、通信が行われるごとに、鍵Ｋを算出することも可能である。

【０２４０】［10.4. 端末装置の別の例］図５２は、実施の形態１０の端末装置の別の構成例を示すブロック図である。この端末装置８６０では、通信回路８６１が受信した受信信号は、低雑音増幅器（Low Noise Amplifier）８６２で増幅され、ＶＣＯ（Voltage Controlled Oscillator；電圧制御型発振器）８６４に結合したミキサ８６３によって復調された後、ベースバンド回路８７８で処理される。また、ベースバンド回路８７８で処理された送信信号は、ＶＣＯ８６６に結合したミキサ８６５で変調され、電力増幅器（Power Amplifier）８６７で増幅された後、通信事業者設備へ送信される。

【０２４１】一方、無線ＬＡＮ回路８７１が受信した受信信号は、低雑音増幅器８７２で増幅され、ＶＣＯ８７４に結合したミキサ８７３によって復調された後、切替回路８７０を経由し、ＶＣＯ８６９に結合したミキサ８６８によって変調される。変調された受信信号は、通信回路８６１のミキサ８６３を経て、ベースバンド回路８７８へ入力される。ベースバンド回路８７８へ入力された無線ＬＡＮの受信信号は、復号化回路８５２によって復号化される。無線ＬＡＮの送信信号は、ベースバンド回路８７８から暗号化回路８５１および切替回路８５６を経て、ベースバンド回路８７９へ入力される。その後、この送信信号は、ＶＣＯ７６６に結合したミキサ８７５で変調され、電力増幅器８７７で増幅された後に送信される。

【０２４２】以上のように、図５２の端末装置８６０は、無線ＬＡＮ回路へ入力された受信信号が復調された後に、変調されて通信回路８６１へ入力される。図５３が示すように、ミキサ８５８は、復調された無線ＬＡＮの受信信号を、通信回路用帯域内に設定された特定範囲（図５３に「特別バンド」と記される）内の周波数ｆを有する搬送波を用いて変調する。このため、無線ＬＡＮの受信信号の周波数ｆが、無線ＬＡＮ回路用帯域内のいずれの範囲にあっても、通信回路８６１には、周波数ｆ

53

が特別バンドの範囲内にある変調波が入力される。

【０２４３】仮に、無線ＬＡＮの受信信号を復調することなく、周波数の変換のみを行って通信回路８６１へ入力した場合には、図５４が示すように、通信回路用バンドを広く確保する必要がある。これに対して、図５２の端末装置８６０では、通信回路用バンドを広く確保する必要がなく、通信回路８６１の周波数帯域の使用効率を高めることができるという利点が得られる。

【０２４４】図４９または図５２に例示されるように、通信回路と無線ＬＡＮ回路とが選択自在に結合した端末装置では、図５５が示すように、通信事業者設備を媒介とした通信経路と無線ＬＡＮとを結合することも可能となる。すなわち、無線ＬＡＮを形成している複数の端末装置８５０ａ～８５０ｃの一部である端末装置８５０ｃの遠距離通信部８４７の通信回路を通じて、別の端末装置８５０ａが通信事業者設備を媒介とした通信を行うことができる。このように、電波が侵入し難い地下街などにある端末装置が、通信事業者設備を媒介した通信を行うことも可能である。通信事業者設備を媒介とした通信経路と無線ＬＡＮとを結合する端末装置（図５５の例では、端末装置８５０ｃ）の負担を軽くするために、このような通信は、緊急非常通信に限って許可してもよい。

【０２４５】また、無線ＬＡＮを通じての通信を、すべて緊急非常通信に制限することも可能である。それによって、無線ＬＡＮを媒介とした通信を中継する端末装置（図４７の例では、端末装置８４０ｂ，８４０ｃ）の負担を軽減することができる。また、緊急非常通信では、通信内容の漏洩に対するセキュリティの重要性が低いので、暗号化のための回路を除去することも可能となる。なお、緊急非常通信とは、例えば生命、財産を脅かす緊急事態の発生にともなう救助の要請などを目的とした通信である。

【０２４６】［11. 実施の形態１１］地下街、ビルディングの中など、通常時には多数の群衆が集中することが想定される領域においても、例えば夜間など時間帯によっては群衆の密度は低減する。実施の形態１１では、電波が侵入し難い領域で、群衆の密度が低い場合にも、無線ＬＡＮを媒介とした通信を可能にする通信方法について説明する。

【０２４７】図５６は、実施の形態による通信方法を示す説明図である。この通信方法では、地下街などの電波が侵入し難い領域に、無線ＬＡＮの形成を可能にする端末装置１０５０ａ、１０５０ｂが設置される。端末装置１０５０ａ、１０５０ｂは、好ましくは公衆電話機であり、例えば地下街の商店の入り口付近に設置される。この場合には、端末装置１０５０ａ、１０５０ｂは、近距離通信部８４８とともに、公衆電話機の本来の機能を達成する遠距離通信部１０５７を備える。群衆の密度が低い場合でも、端末装置８５０ａと端末装置８５０ｂとが、端末装置１０５０ａ、１０５０ｂの近距離通信部８４８を中継することにより、無線ＬＡＮを媒介した通信を行うことができる。

54

【０２４８】［12. 実施の形態１２］実施の形態１２では、以上の実施の形態で説明した半導体素子４０１、符号化回路４０２および比較回路４０３に関し、さらに望ましい形態について説明する。

【０２４９】［12.1. 半導体素子の例］図５７は、半導体素子４０１の好ましい一例を示す回路図である。この半導体素子４０１ａは、基板の上にマトリクス状に配列された複数の（図５７の例では、４×４個＝１６個の）TFT１０１を備えている。基板の上には、さらに、複数のワード線ＷＬ１～ＷＬ４、および、複数のビット線ＢＬ１～ＢＬ４が、それぞれ、横方向および縦方向に配列されている。

【０２５０】ワード線ＷＬ１～ＷＬ４の各々には、図上横一列に配列する４個のTFT１０１のゲート電極が共通に接続されている。一方、ビット線ＢＬ１～ＢＬ４の各々には、図上縦一列に配列する４個のTFT１０１のドレイン電極が共通に接続されている。１６個のTFT１０１のソース電極は、正電源線へ共通に接続されている。また、ビット線ＢＬ１～ＢＬ４の各々の一端はビット線負荷７を通じて接地電源線へ接続されている。

【０２５１】ビット線負荷７の接地線とは反対側の一端には、アナログ信号Anを取り出すための配線１８が接続されている。さらに、ビット線ＢＬ１～ＢＬ４の各々の他端には、パッド１５が接続されており、ワード線ＷＬ１～ＷＬ４の各々の一端には、パッド１６が接続されている。

【０２５２】半導体素子４０１ａは、以上のように構成されるので、ワード線ＷＬ１～ＷＬ４の中の一つに、所定の高さのゲート電圧を付与することにより、そのワード線に接続された４個のTFT１０１に、ドレイン電流Id1～Id4が、それぞれ流れる。ドレイン電流Id1～Id4は、それぞれ、ビット線負荷１７を流れるので、ビット線ＢＬ１～ＢＬ４に接続された配線１８には、ドレイン電流Id1～Id4に比例した電位が発生する。この４個の電位がアナログ信号Anとして外部へ出力される。ワード線ＷＬ１～ＷＬ４に、順次、ゲート電圧を付与することにより、合計１６個の電位を、アナログ信号Anとして取り出すことができる。

【０２５３】１６個のアナログ信号Anは、符号化回路４０２によって符号化されることにより、例えば、図５８が例示するように、１６ビットのデジタル信号へ変換される。図５８は、符号のもとになるTFT１０１と、それに接続されるビット線ＢＬ１～ＢＬ４およびワード線ＷＬ１～ＷＬ４との関係がわかるように、１６ビットの符号をマトリクス状に配列して示している。

【０２５４】［12.2. 符号化回路および比較回路の例］図５９は、図１に示した半導体基板ＣＨ３（またはＣＨ１）を半導体基板とする半導体装置の好ましい形態を示

55

すブロック図である。この半導体装置４０４ａは、図５７に示した半導体素子４０１ａを備えている。半導体装置４０４ａには、半導体素子４０１ａに備わる複数のワード線ＷＬ１～ＷＬ４の任意の一つを、アドレス信号Adrにもとづいて駆動するデコーダ・ドライバ４１０が備わっている。アドレス信号Adrは、入力端子を通じて外部から入力することが可能である。

【０２５５】また、符号化回路４０２が出力する符号Cdは、比較回路４０３へ入力されるだけでなく、バッファ回路４１１を介して、外部へも出力される。それにより、限られた範囲の者が、識別符号Ｃｄをあらかじめ知ることが可能となる。バッファ回路４１１が備わるので、符号化回路４０２が出力する識別符号Ｃｄとは異なる符号を、識別符号Ｃｄの出力端子を通じて外部から比較回路４０３へ入力するという不正行為を防止することができる。

【０２５６】半導体素子４０１ａには、パッド１５，１６が備わるので、半導体装置４０４ａを製造する過程の中では、これらのパッド１５，１６に探針を当てることにより、アナログ信号Anを直接に読み出すことも可能である。読み出されたアナログ信号Anは、符号化回路４０２と同一の特性を持った装置を用いて、識別符号Ｃｄへと変換することができ、それにより、識別符号Ｃｄを得ることも可能である。したがって、識別符号Ｃｄの読み出しが、半導体装置４０４ａの製造工場以外で行われる必要がなければ、アドレス信号Adrの入力端子、識別符号Ｃｄの出力端子、および、バッファ回路４１１は、除去してもよい。

【０２５７】比較回路４０３は、入力端子を通じて入力される記憶符号Ｃｏを、識別符号Ｃｄと比較する際に、デコーダ・ドライバ４１０へ、アドレス信号Adrを入力する。それにより、半導体装置４０４ａが駆動され、アナログ信号Anが読み出されるので、外部からアドレス信号Adrを入力しなくても、識別符号Ｃｄと記憶符号Ｃｏとの間の比較を行うことが可能となる。

【０２５８】図６０は、符号化回路４０２の好ましい形態を示す回路図であり、代表としてビット線ＢＬ１に接続される部分を描いている。他のビット線ＢＬ２～ＢＬ４にも、図６０と同様の回路部分が接続されている。この符号化回路４０２ａには、センスアンプ１９０が備わっている。センスアンプ１９０は、配線１８の電位と、トランジスタ１９２，１９３が生成する基準電位Vrefとを比較して、ハイレベルまたはロウレベルの信号を生成し、識別符号Ｃｄの１ビット分（例えば、ビット線ＢＬ１に対応した識別符号Ｃｄ(1)）として出力する。

【０２５９】センスアンプ１９０では、NMOSトランジスタ１９４とPMOSトランジスタ１９５の直列回路、および、NMOSトランジスタ１９６とPMOSトランジスタ１９７の直列回路が、接地電源線と正電源線との間に介挿されている。そして、PMOSトランジスタ１９５のゲート電極

56

とドレイン電極、および、PMOSトランジスタ１９７のゲート電極が、互いに接続されることにより、カレントミラー回路が形成されている。

【０２６０】TFT１０１を流れるドレイン電流は、約１ｐＡ（10^{-12}Ａ）～約１μＡの範囲内の低い値である。したがって、ビット線負荷１７として、NMOSトランジスタを用い、そのゲート電極に一定電位を印加することによって、そのドレイン電流を、約１ｎＡ（10^{-9}Ａ）程度に設定するのが望ましい。それによって、センスアンプ１９０の感度が高められる。ドレイン電流を約１ｎＡ程度に設定する上で、ゲート電位は、接地電位とするのが望ましい。

【０２６１】NMOSトランジスタ１９２とPMOSトランジスタ１９３の直列回路が、接地電源線と正電源線との間に介挿されており、これらの二つのトランジスタの接続部から基準電位Vrefが取り出される。NMOSトランジスタ１９２およびPMOSトランジスタ１９３のゲート電極には、それぞれ接地電源線の電位および正電源線の電位などの一定電位が供給される。配線１８の電位と基準電離Vrefとが比較されることは、TFT１０１のドレイン電流とNMOSトランジスタ１９２とPMOSトランジスタ１９３の直列回路を流れる基準電流Ir（またはその定数倍）とが比較されることと等価である。

【０２６２】安定した比較を行う上では、図６０に描かれるTFT１０１以外のトランジスタは、TFT型ではないバルク型のトランジスタとして構成されるのが望ましい。TFT１０１以外のトランジスタを、TFT１０１と同じく多結晶TFTとして形成するのであれば、それらのドレイン電流の大きさを安定なものとするために、それらのゲート長およびゲート幅は、TFT１０１のゲート長およびゲート幅よりも大きく設定されるのが望ましい。

【０２６３】［12.3. 半導体素子の別の例］半導体素子４０１は、多結晶型のTFT１０１を備える代わりに、例えば、多結晶体の抵抗素子、あるいは、多結晶体のキャパシタ（容量素子）を備えてもよい。以下では、そのような例について説明する。

【０２６４】図６１は、半導体素子４０１が多結晶体の抵抗素子を備える例を示す回路図である。この半導体素子４０１ｂでは、基板の上にマトリクス状に配列された複数の（図６１の例では、４×４個＝１６個の）抵抗素子４３を備えている。抵抗素子４３では、その抵抗体が、多結晶半導体、例えば多結晶シリコンで形成されている。このため、抵抗素子４３では、抵抗値がランダムにばらつく。

【０２６５】基板の上には、さらに、複数のワード線ＷＬ１～ＷＬ４、および、複数のビット線ＢＬ１～ＢＬ４が、それぞれ横方向および縦方向に配列されている。

【０２６６】ワード線ＷＬ１～ＷＬ４の各々には、図上横一列に配列する４個の抵抗素子４３の一端が共通に接続されている。一方、ビット線ＢＬ１～ＢＬ４の各々に

57

は、図上縦一列に配列する４個の抵抗素子４３の他端が共通に接続されている。また、ビット線ＢＬ１～ＢＬ４の各々の一端はビット線負荷としてのNMOSトランジスタ４８を通じて接地電源線へ接続されている。NMOSトランジスタ４８のゲート電極は、例えば、接地電源線に接続される。

【０２６７】NMOSトランジスタ４８のドレイン電極には、アナログ信号Anを取り出すための配線４９が接続されている。さらに、ビット線ＢＬ１～ＢＬ４の各々の他端には、パッド１５が接続されており、ワード線ＷＬ１～ＷＬ４の各々の一端には、パッド１６が接続されている。

【０２６８】半導体素子４０１ｂは、以上のように構成されるので、ワード線ＷＬ１～ＷＬ４の中の一つに、所定の高さのゲート電圧を付与することにより、そのワード線に接続された４個の抵抗素子４３に電流が流れる。これらの電流は、NMOSトランジスタ４８を流れるので、ビット線ＢＬ１～ＢＬ４に接続された配線４９の各々には、抵抗素子４３を流れる電流に比例した電位が発生する。この４個の電位がアナログ信号Anとして外部へ出力される。ワード線ＷＬ１～ＷＬ４に、順次、所定の電位を付与することにより、合計１６個の電位を、アナログ信号Anとして取り出すことができる。アナログ信号Anは、抵抗素子４３の抵抗のばらつきに対応したランダムな値として得られる。

【０２６９】パッド１５，１６が備わるので、探針を用いて半導体素子４０１ｂの製造工程の中で、アナログ信号Anを読み出すことも可能である。また、抵抗素子４３は、一次元マトリクス状に配列され、すべての抵抗素子４３の一端が単一のワード線に接続されてもよい。アナログ信号Anのばらつきを大きくするためには、抵抗素子４３が有する多結晶体の長さおよび幅を、ゲート長Ｌおよびゲート幅Ｗに対する最適条件と同様の範囲に設定するとよい。

【０２７０】［12.4. 半導体素子のさらに別の例］図６２は、半導体素子４０１が多結晶体の容量素子を備える例を示す回路図である。この半導体素子４０１ｃでは、基板の上にマトリクス状に配列された複数の（図６１の例では、４×４個＝１６個の）容量素子９１とMOSトランジスタ９０の直列回路を備えている。容量素子９１には、多結晶誘電体、例えばＢＳＴ（$Ba_xSr_{1-x}TiO_3$）などのペロブスカイト型の多結晶誘電体が備わっている。このため、容量素子９１では、容量値がランダムにばらつく。

【０２７１】基板の上には、さらに、複数のワード線ＷＬ１～ＷＬ４、および、複数のビット線ＢＬ１～ＢＬ４が、それぞれ横方向および縦方向に配列されている。ワード線ＷＬ１～ＷＬ４の各々には、図上横一列に配列する４個の直列回路に属するMOSトランジスタ９０のゲート電極が共通に接続されている。一方、ビット線ＢＬ１～ＢＬ４の各々には、図上縦一列に配列する４個の直列回路に属するMOSトランジスタ９０のソース電極およびドレイン電極の一方電極が、共通に接続されている。１６個の直列回路に属する容量素子９１の一端は、接地電源線に接続されている。ビット線ＢＬ１～ＢＬ４の各々の他端には、パッド１５が接続されており、ワード線ＷＬ１～ＷＬ４の各々の一端には、パッド１６が接続されている。

58

【０２７２】半導体素子４０１ｃは、以上のように構成されるので、ワード線ＷＬ１～ＷＬ４の中の一つに、所定の高さのゲート電圧を付与することにより、そのワード線に接続された４個のMOSトランジスタをオンさせることができる。オンしたMOSトランジスタを通じて、４個の容量素子９１の他端が、ビット線ＢＬ１～ＢＬ４に電気的に接続される。このときビット線ＢＬ１～ＢＬ４を通じて、４個の容量素子９１の容量（キャパシタンス）を計測することができる。例えば、一定時間にわたって電流を供給したときの電位を計測することができ、この電位をアナログ信号Anとして取り出すとよい。この電位には、容量素子９１の容量が反映されている。

【０２７３】ワード線ＷＬ１～ＷＬ４に、順次、所定のゲート電圧を付与することにより、合計１６個の電位を、アナログ信号Anとして取り出すことができる。アナログ信号Anは、容量素子９１の容量のばらつきに対応したランダムな値として得られる。パッド１５，１６が備わるので、探針を用いて半導体素子４０１ｃの製造工程の中で、アナログ信号Anを読み出すことも可能である。また、容量素子９１とMOSトランジスタ９０との直列回路は、一次元マトリクス状に配列され、すべてのMOSトランジスタ９０のゲート電極が単一のワード線に接続されてもよい。

【０２７４】アナログ信号Anのばらつきを大きくするためには、容量素子９１が有する多結晶誘電体の長さおよび幅を、ゲート長Ｌおよびゲート幅Ｗに対する最適条件と同様の範囲に設定するとよい。ＢＳＴでは、その膜厚が100nmであるとき、シリコン酸化膜に換算した膜厚は、約0.5nmである。したがって、電極に面するＢＳＴの形状が、一辺が0.3μmの正方形であるとすると、その容量は6.2fF程度となる。結晶粒径（平均値）が膜厚に相当する100nmに設定された最適な場合では、その容量は−30%～+30%の範囲、すなわち、4.3fF～8.1fFの範囲にばらつく。この値は、識別として利用するのに十分な大きさのばらつきであると云える。

【０２７５】［12.5. 比較回路のさらに別の例］図６３は、図１に示した半導体基板ＣＨ３（またはＣＨ１）を半導体基板とする半導体装置の好ましい別の形態を示すブロック図である。この半導体装置４０４ｄが備える比較回路４０３ａは、識別符号Ｃｄと記憶符号Ｃｏとの完全一致性だけでなく、あらかじめ定められた範囲での近似性をも判定することができるように構成されている。

判定の基準値SLは、入力端子を通じて半導体装置４０４ｄの外部から入力することができる。

【０２７６】このことを可能にするために、比較回路４０３ａは、ワード線ＷＬの電位をスイープするスイープ回路２００を備えている。ワード線ＷＬの電位がスイープされることによって変化する識別符号Ｃｄは、近似度算出回路１９９によって、入力符号メモリ１９８に保持される記憶符号Ｃｏの対応する一部と比較される。近似度算出回路１９９は、比較を通じて算出した双方の符号の間の近似度VAを、評価回路２１０へ伝達する。評価回路２１０は、近似度VAを基準値SLと比較することによって、近似度VAが一定以上であるか否かを判定し、その結果を判定信号VBとして出力する。

【０２７７】判定信号VBは、デコーダ・ドライバ４１０が駆動する一つのワード線ＷＬごとに個別に得られる。アドレス発生回路４４１は、すべてのワード線ＷＬを、一つずつ順に指定するアドレス信号をデコーダ・ドライバ４１０へ伝達する。それにより、すべてのワード線ＷＬに対応した複数の判定信号VBが、一つずつ順に得られる。

【０２７８】総合判定回路２２０は、すべてのワード線ＷＬに対応した複数の判定信号VBにもとづいて、すべてのワード線ＷＬに対応した全ビットの符号Cdと、全ビットの符号Coとの間の近似性を判定し、その結果を表現する判定信号Ｅｎを出力する。基準値SLを適切に設定することにより、近似性の判定として、もっとも厳しい完全一致性の判定を選択することも可能である。ワード線が単一であれば、総合判定回路２２０は不要であり、判定信号VBがそのまま判定信号Ｅｎとして出力される。

【０２７９】制御回路４４２は、入力端子を通じて入力される指示信号Stに応答して、比較回路４０３ａの各要素の動作を開始させるとともに、各要素の動作を所定の手順に沿うように制御する。特に、制御回路４４２からスイープ回路２００へと、スイープを行うか否かを指示する制御信号であるスイープスイッチ信号SSが伝達される。なお、近似度算出回路１９９、評価回路２１０、および、総合判定回路２２０は、判定回路４４０を構成する。

【０２８０】

【発明の効果】第１の発明の装置では、半導体基板を識別するための符号が、別の半導体基板に記憶されているので、本装置が組み込まれた応用機器を、半導体基板を取り替えて使用するという不正行為を、これらの符号を照合することによって防止することができる。

【０２８１】第２の発明の装置では、メモリがＯＴＰＲＯＭに符号を記憶するので、メモリに記憶される符号の不正な変更に対する障壁が高い。

【０２８２】第３の発明の装置では、半導体素子の電気的特性のばらつきを利用して識別符号が生成されるので、量産される多数の本装置の間で、同一工程で製造された半導体素子を用いることができる。このため、装置の製造が簡略化される。また、識別符号のもとになる半導体素子の電気的特性を外部から変更することができないので、識別符号の不正な変更に対する障壁が高い。

【０２８３】第４の発明の装置では、半導体素子が多結晶体を有し、その結晶構造のばらつきを利用して識別符号が生成されるので、同一工程で製造された半導体素子の間での電気的特性のばらつきが大きい。このため、量産される多数の本装置の間で、互いに識別符号が一致しないようにすることが容易である。

【０２８４】第５の発明の装置では、符号生成部がＯＴＰＲＯＭに識別符号を記憶するので、符号生成部が生成する識別符号の不正な変更に対する障壁が高い。

【０２８５】第６の発明の装置では、比較回路によって、符号の一致性の判定が行われるので、判定信号を認証に利用することができる。

【０２８６】第７の発明の装置では、符号生成部が形成されている半導体基板に比較回路が形成されているので、同一の半導体基板の中で符号生成部から比較回路へ入力される識別符号を外部から不正に変更することができない。このため、不正使用に対する障壁が、さらに高められる。

【０２８７】第８の発明の装置では、異なる半導体基板の間で、暗号化された形式で符号がやりとりされるので、外部から符号を読み取ることができない。このため、不正使用に対する障壁がさらに高められる。

【０２８８】第９の発明の装置では、半導体素子の電気的特性のばらつきを利用して鍵が生成されるので、量産される多数の本装置の間で、同一工程で製造された半導体素子を用いることができる。このため、装置の製造が簡略化される。また、鍵のもとになる半導体素子の電気的特性を外部から変更することができないので、鍵の不正な変更に対する障壁が高い。

【０２８９】第１０の発明の装置では、半導体素子が多結晶体を有し、その結晶構造のばらつきを利用して鍵が生成されるので、同一工程で製造された半導体素子の間での電気的特性のばらつきが大きい。このため、量産される多数の本装置の間で、互いに鍵が一致しないようにすることが容易である。

【０２９０】第１１の発明の装置では、鍵生成部が、ＯＴＰＲＯＭに鍵を記憶するので、鍵生成部が生成する鍵の不正な変更に対する障壁が高い。

【０２９１】第１２の発明の装置では、スイッチ回路が備わるので、半導体基板から出力される識別符号を記憶符号に見せかけて、そのまま同一の半導体基板へ入力することによってなされる不正使用を防止することができる。

【０２９２】第１３の発明の装置では、比較回路の判定にもとづいて動作または非動作となる回路部分を含む所定回路が備わるので、所定回路を応用機器の機能を実現

する回路の一部とすることにより、比較の結果に応じて、応用機器の所定の動作を許可および不許可することができる。

【０２９３】第１４の発明の装置では、符号生成部および比較回路が形成されている半導体基板の一つに所定回路が形成されているので、同一の半導体基板の中で比較回路から所定回路へ入力される判定信号については、これを外部から入力することができない。このため、不正使用に対する障壁が、さらに高められる。

【０２９４】第１５の発明の装置では、二つの半導体基板の一方に符号生成部が形成され、他方にメモリが形成され、一方の半導体基板に固有の識別符号に一致する符号が他方の半導体基板に記憶されるという、もっとも簡素な構成を有する。このため、装置の製造が容易であり、かつ装置を小型化することが可能である。

【０２９５】第１６の発明の装置では、二つの半導体基板のいずれにも符号生成部とメモリとが形成され、二つの半導体基板が、互いに相手側の識別符号に一致する符号を記憶するので、半導体基板の個数を最小に抑えつつ、不正使用に対する障壁をさらに高めることができる。

【０２９６】第１７の発明の装置では、暗号化した形式でデータを外部との間でやりとりすることができるので、データが表現する情報の漏洩に対する障壁が高い。しかも、半導体素子の電気的特性のばらつきを利用して暗号化のための鍵が生成されるので、量産される多数の本装置の間で、同一工程で製造された半導体素子を用いることができる。このため、装置の製造が簡略化される。また、鍵のもとになる半導体素子の電気的特性を外部から変更することができないので、鍵の不正な変更に対する障壁が高い。

【０２９７】第１８の発明の装置では、本体部に着脱自在の補助部に鍵生成部が組み込まれているので、複数の本体部に対して同一の鍵を使用することが可能である。

【０２９８】第１９の発明の装置では、鍵生成部がＩＣカードに組み込まれているので、携帯に便利である。

【０２９９】第２０の発明の装置では、半導体素子が多結晶体を有し、その結晶構造のばらつきを利用して鍵が生成されるので、同一工程で製造された半導体素子の間での電気的特性のばらつきが大きい。このため、量産される多数の本装置の間で、互いに鍵が一致しないようにすることが容易である。

【０３００】第２１の発明の装置では、比較回路の判定が不一致を示すときに送信または受信の少なくとも一方を停止する通信回路が備わるので、半導体基板を取り替えて通信に使用するという不正行為が、通信事業者設備等による処理を待つことなく端末装置自体の働きによって自動的に抑えられる。

【０３０１】第２２の発明の装置では、各判定信号が送信されるので、通信事業者設備等が判定信号にもとづいて認証処理を行うことにより、半導体基板を取り替えて通信に使用するという不正行為を防止することができる。

【０３０２】第２３の発明の装置では、各識別符号と各記憶符号とが送信されるので、通信事業者設備等がこれらの符号を比較し、その結果にもとづいて認証処理を行うことにより、半導体基板を取り替えて通信に使用するという不正行為を防止することができる。

【０３０３】第２４の発明の装置では、本体部に着脱自在の補助部にメモリが組み込まれているので、本体部と補助部とが結合したとき、および結合していないときの二通りの間で異なるレベルでの認証を通信事業者設備等が行うことができる。例えば、通信事業者設備は、本体部と補助部とが結合したときの高レベルの認証によって、それ以前の通信に対する通信料金を、裏付けられたものとして記録することができ、それにより端末装置の紛失を装って料金支払いの義務を逃れる違法行為を防止することが可能となる。

【０３０４】第２５の発明の装置では、暗号化された形式で、識別符号および記憶符号が送信されるので、これらの符号の漏洩に対する障壁が高い。

【０３０５】第２６の発明の装置では、第１鍵生成部と第１暗号化回路とが、符号化回路とともに単一の半導体基板に形成されているので、識別符号および第１鍵の漏洩に対する障壁がさらに高められる。

【０３０６】第２７の発明の装置では、第２鍵生成部と第２暗号化回路とが、メモリとともに単一の半導体基板に形成されているので、記憶符号および第２鍵の漏洩に対する障壁がさらに高められる。

【０３０７】第２８の発明の装置では、補助部が本体部の電池を充電する充電器であるので、使用者に特別の手間を要求することなく、本体部と補助部との結合が定期的に行われる。

【０３０８】第２９の発明の装置では、補助部がＩＣカードでありので、携帯に便利である。また、本体部と補助部の間で、無線で符号がやり取りされるので、ＩＣカードを本体部とともに携帯するだけで、双方の結合が実現する。

【０３０９】第３０の発明の装置では、符号生成部が形成されている半導体基板の一つに通信回路が形成されているので、同一の半導体基板の中で通信回路へ入力される判定信号または符号については、これを外部から入力することができない。このため、不正使用に対する障壁が、さらに高められる。

【０３１０】第３１の発明の装置では、本装置を携帯する群衆が集合ないし通行する空間において、群衆の中の少なくとも一部の複数人が携帯する本装置の間で無線通信網を形成することができ、それにより、通信事業者設備を媒介した無線通信を行い得ない領域、例えば地下街などが上記空間の中にあっても、上記空間の中での通信

が可能となる。

【０３１１】第３２の発明の装置では、切替回路が備わるので、無線通信網を通じての他者どうしの通信が中継されるだけでなく、本装置の使用者自身が無線通信網による通信を行うことができる。

【０３１２】第３３の発明の装置では、通信相手と符号を交換することにより共通鍵が設定され、当該共通鍵にもとづいて暗号化された形式で通信信号がやりとりされるので、任意の通信相手との通信内容の漏洩に対する障壁が高い。

【０３１３】第３４の発明の装置では、半導体素子の電気的特性のばらつきを利用して、共通鍵のもとになる符号が生成されるので、量産される多数の本装置の間で、同一工程で製造された半導体素子を用いることができる。このため、装置の製造が簡略化される。また、符号のもとになる半導体素子の電気的特性を外部から変更することができないので、符号の不正な変更に対する障壁が高い。

【０３１４】第３５の発明の装置では、半導体素子が多結晶体を有し、その結晶構造のばらつきを利用して符号が生成されるので、同一工程で製造された半導体素子の間での電気的特性のばらつきが大きい。このため、量産される多数の本装置の間で、互いに符号が一致しないようにすることが容易である。

【０３１５】第３６の発明の装置では、符号生成部がＯＴＰＲＯＭに符号を記憶するので、符号生成部が生成する符号の不正な変更に対する障壁が高い。

【０３１６】第３７の発明の装置では、無線通信網回路が受信した信号が、復調された後に変調されて通信回路へ伝えられるので、通信回路の周波数帯域の使用効率が高められる。

【０３１７】第３８の発明の方法では、端末装置が送信する各判定信号が認証に用いられるので、半導体基板を取り替えて通信に使用するという不正行為を防止することができる。

【０３１８】第３９の発明の方法では、端末装置が送信する各識別符号および各記憶符号が認証に用いられるので、半導体基板を取り替えて通信に使用するという不正行為を防止することができる。

【０３１９】第４０の発明の方法では、受信した各識別符号および各記憶符号が記録されるので、不正使用による犯罪を事前に抑止する効果が得られる。また、不正使用があった場合に、記録している各符号を不正使用者の特定に役立てることが可能となる。

【０３２０】第４１の発明の方法では、認証工程で認証を行わない場合、すなわち使用者が不正使用者である可能性のある場合に、受信した各識別符号および各記憶符号が記録されるので、記録した各符号を不正使用者の特定に役立てることができる。

【０３２１】第４２の発明の方法では、本体部と補助部とが結合したとき、および結合していないときの二通りの間で異なるレベルでの認証が行われる。本体部と補助部とが結合したときになされる高位の認証は、識別符号と記憶符号のいずれもが、登録された符号と一致する場合に限ってなされるので、端末装置が正当に使用されている確度がより高いことを証明するものとなる。したがって、通信事業者設備は、手続の重要性に応じた認証を使い分けることが可能となる。

【０３２２】第４３の発明の方法では、補助部が本体部に装着された状態で通信を行うことにより、登録すべき記憶符号が通信事業者設備へ送られるので、端末装置が使用者の手に渡るより前には、識別符号のみを登録すれば足りる。

【０３２３】第４４の発明の方法では、第２登録符号を変更することが可能であるので、使用者は、端末装置を入手後に必要に応じて補助部を交換することができる。

【０３２４】第４５の発明の方法では、本体部と補助部とが結合したとき、および結合していないときの二通りの間で異なるレベルでの認証が行われる。本体部と補助部とが結合したときになされる高位の認証は、識別符号と記憶符号のいずれもが、登録された符号と一致する場合に限ってなされるので、端末装置が正当に使用されている確度がより高いことを証明するものとなる。したがって、通信事業者設備は、手続の重要性に応じた認証を使い分けることが可能となる。しかも、暗号化された形式で、識別符号および記憶符号が送信されるので、これらの符号の漏洩に対する障壁が高い。

【０３２５】第４６の発明の方法では、補助部が本体部に装着された状態で通信を行うことにより、登録すべき記憶符号が通信事業者設備へ送られるので、端末装置が使用者の手に渡るより前には、識別符号のみを登録すれば足りる。

【０３２６】第４７の発明の方法では、第２登録符号を変更することが可能であるので、使用者は、端末装置を入手後に必要に応じて補助部を交換することができる。

【０３２７】第４８の発明の方法では、高位の認証工程で認証を行わない場合、すなわち使用者が不正使用者である可能性が高い場合に、受信した各識別符号および各記憶符号が記録されるので、記録した各符号を不正使用者の特定に役立てることができる。

【０３２８】第４９の発明の方法では、高位認証工程において、高位の認証を行う場合、すなわち、使用者が正当使用者である可能性が高い場合には、それ以前の通信に対する通信料金を、裏付けられたものとして記録するので、端末装置の紛失を装って料金支払いの義務を逃れる違法行為を防止することが可能である。

【０３２９】第５０の発明の方法では、補助部が本体部に装着されない状態でなされる通常の認証に、過去の高位の認証工程でなされた判断結果が反映されるので、商取引などの重要な手続を、通常の認証の下で行うことが

65

できる。

【０３３０】第５１の発明の方法では、高位認証工程において、それ以前の通信によって行われた商取引の成立または不成立が、高位の認証を行うか否かに応じて記録されるので、端末装置の不正使用にもとづく不正な商取引による損害を解消ないし低減することができる。

【０３３１】第５２の発明の方法では、認証工程において、認証を行うか否かに応じて通信が継続または中止されるので、端末装置の不正使用にもとづく通信を防止することができる。

【０３３２】第５３の発明の方法では、所定の機能を有する端末装置を携帯する群衆が集合ないし通行する空間において、群衆の中の少なくとも一部の複数人が携帯する上記端末装置の間で無線通信網が形成され、それにより、通信事業者設備を媒介した無線通信を行い得ない領域、例えば地下街などが上記空間の中にあっても、上記空間の中での通信が実現する。

【０３３３】第５４の発明の方法では、無線通信網を形成する複数の端末装置の一部が通信事業者設備を媒介した無線通信を行うことにより、上記複数の端末装置の他の一部が無線通信網と通信事業者設備とを媒介した通信を行うことが可能であるので、通信事業者設備を媒介した無線通信を行い得ない領域、例えば地下街などから、通信事業者設備を媒介した無線通信を行うことが可能となる。

【０３３４】第５５の発明の方法では、通信相手と符号を交換することにより共通鍵が設定され、当該共通鍵にもとづいて暗号化された形式で通信信号がやりとりされるので、任意の通信相手との通信内容の漏洩に対する障壁が高い。

【０３３５】第５６の発明の方法では、無線通信網を媒介した通信が、例えば生命、財産を脅かす緊急事態の発生にともなう救助の要請などの、緊急非常通信に限って可能とされるので、通信内容の漏洩を防止するための暗号化などの手順を要しない。

【０３３６】第５７の発明の方法では、無線通信網の形成が可能な端末装置が、通信事業者設備を媒介した無線通信を行い得ない領域、例えば地下街などに設置されるので、上記領域において、所定の機能を有する端末装置を携帯する群衆の密度が低い場合でも、無線通信網を媒介した通信が可能となる。

【図面の簡単な説明】

【図１】　実施の形態１の半導体装置のブロック図である。

【図２】　図１の符号生成部のブロック図である。

【図３】　図２の半導体素子の平面図である。

【図４】　図３の半導体素子のＡ－Ａ切断線に沿った断面図である。

【図５】　図２の半導体素子の平面図である。

【図６】　図２の半導体素子の特性を表すグラフである。

66

【図７】　図１の符号生成部の別の例のブロック図である。

【図８】　図１のメモリのブロック図である。

【図９】　実施の形態１の端末装置のブロック図である。

【図１０】　図９の通信回路のブロック図である。

【図１１】　図９の端末装置の使用に至るまでの手順の流れ図である。

【図１２】　実施の形態１の通信システムのブロック図である。

【図１３】　実施の形態２の半導体装置のブロック図である。

【図１４】　実施の形態２の端末装置のブロック図である。

【図１５】　図１３の端末装置の使用に至るまでの手順の流れ図である。

【図１６】　実施の形態３の端末装置のブロック図である。

【図１７】　図１６の端末装置を用いた通信方法の流れ図である。

【図１８】　実施の形態３の端末装置の別の例のブロック図である。

【図１９】　図１８の端末装置を用いた通信方法の流れ図である。

【図２０】　実施の形態４の端末装置のブロック図である。

【図２１】　図２０の端末装置を用いた通信方法の流れ図である。

【図２２】　実施の形態４の端末装置の別の例のブロック図である。

【図２３】　図２２の端末装置を用いた通信方法の流れ図である。

【図２４】　実施の形態５の半導体装置のブロック図である。

【図２５】　図２４の鍵生成部のブロック図である。

【図２６】　図２４の鍵生成部の別の例のブロック図である。

【図２７】　図２４の半導体装置を組み込んだ端末装置の使用に至るまでの手順の流れ図である。

【図２８】　実施の形態５の半導体装置の別の例のブロック図である。

【図２９】　図２８の半導体装置を組み込んだ端末装置の使用に至るまでの手順の流れ図である。

【図３０】　実施の形態６の半導体装置のブロック図である。

【図３１】　実施の形態７の端末装置のブロック図である。

【図３２】　実施の形態７の端末装置の別の例のブロック図である。

67

【図３３】 実施の形態８の端末装置のブロック図である。

【図３４】 図３３の端末装置の使用に至るまでの手順の流れ図である。

【図３５】 図３４のステップＳ５０９の流れ図である。

【図３６】 図３４のステップＳ５０９の流れ図である。

【図３７】 実施の形態９の端末装置のブロック図である。

【図３８】 図３７の端末装置の使用に至るまでの手順の流れ図である。

【図３９】 図３８のステップＳ７０９の流れ図である。

【図４０】 図３８のステップＳ７０９の流れ図である。

【図４１】 図３８のステップＳ７０９の別の例の流れ図である。

【図４２】 図４１のステップＳ７４２の流れ図である。

【図４３】 図４１のステップＳ７４２の流れ図である。

【図４４】 図３８のステップＳ７０９の別の例の流れ図である。

【図４５】 図３８のステップＳ７０９の別の例の流れ図である。

【図４６】 実施の形態９の端末装置の別の例のブロック図である。

【図４７】 実施の形態１０の通信方法の説明図である。

【図４８】 実施の形態１０の端末装置のブロック図である。

【図４９】 実施の形態１０の端末装置の別の例のブロック図である。

【図５０】 図４９の鍵生成部のブロック図である。

【図５１】 図４９の端末装置による鍵生成の流れ図である。

【図５２】 実施の形態１０の端末装置のさらに別の例のブロック図である。

【図５３】 図５２の端末装置の動作説明図である。

68

【図５４】 図５３に対比される動作を示す説明図である。

【図５５】 実施の形態１０の通信方法の別の例の説明図である。

【図５６】 実施の形態１１の通信方法の説明図である。

【図５７】 実施の形態１２の半導体素子のブロック図である。

【図５８】 図５７の半導体素子の動作説明図である。

【図５９】 実施の形態１２の半導体装置のブロック図である。

【図６０】 図５９の符号化回路の一部のブロック図である。

【図６１】 実施の形態１２の半導体素子の別の例のブロック図である。

【図６２】 実施の形態１２の半導体素子のさらに別の例のブロック図である。

【図６３】 実施の形態１２の半導体素子の比較回路のブロック図である。

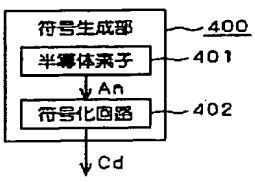
【図６４】 従来の通信システムの処理を説明する図である。

【図６５】 従来の通信端末のブロック図である。

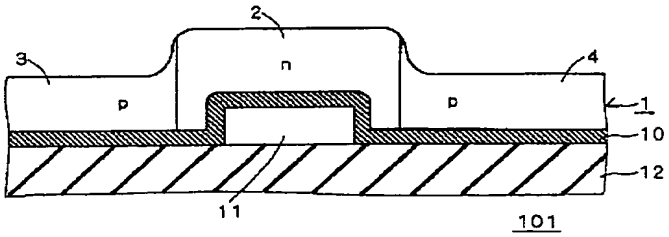
【符号の説明】

４００ 符号生成部、４０１ 半導体素子、４０２ 符号化回路、４０３ 比較回路、４０５，４０５ａ 所定回路、６０１，６５４ メモリ、６０２ ＯＴＰＲＯＭ、６３３，６７６，８５３ 鍵生成部、６３１，８５１ 暗号化回路、６３２，８５２ 復号化回路、６４１ スイッチ回路、６５２，６７２，８２８，６９２ 本体部、６５３，６７３，６９３ 充電器（補助部）、６５５，６７５ 通信事業者設備、６９４，６９５ 通信インタフェース、８２９ ＩＣカード（補助部）、８４１，８６１ 通信回路、８４６，８７１ 無線ＬＡＮ回路（無線通信網回路）、８５６，８７０ 切替回路、８５７ 鍵演算部、８６８，８７３ ミキサ、Ｃｄ，Ｃｄ１，Ｃｄ２ 識別符号、Ｃｏ，Ｃｏ１，Ｃｏ２ 記憶符号、ＣＨ１～ＣＨ６，ＣＨ１０～ＣＨ１３，ＣＨ２０～ＣＨ２３，ＣＨ４０～ＣＨ４２，ＣＨ５０～ＣＨ５２，ＣＨ７０，ＣＨ７１，ＣＨ９０～ＣＨ９２，ＣＨ１００～ＣＨ１０４ 半導体基板、Ｋ，Ｋ１，Ｋ２ 鍵。

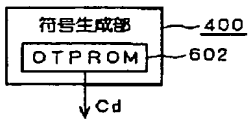
【図２】



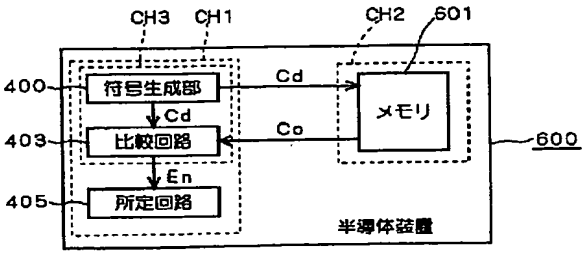
【図４】



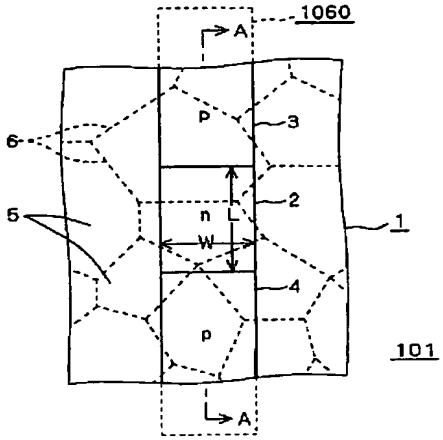
【図７】



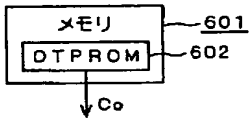
【図１】



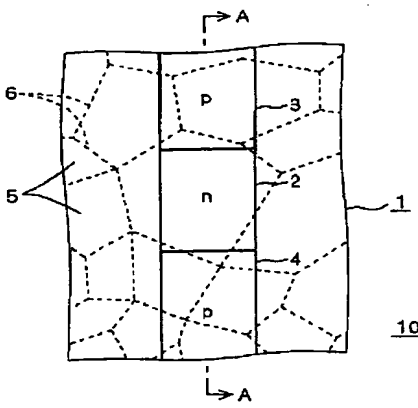
【図３】



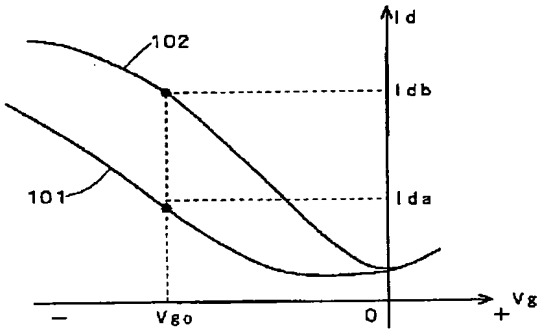
【図８】



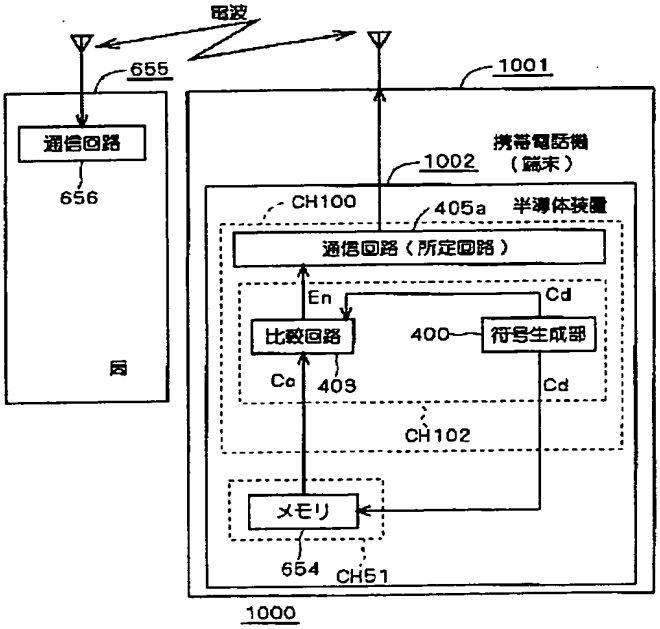
【図５】



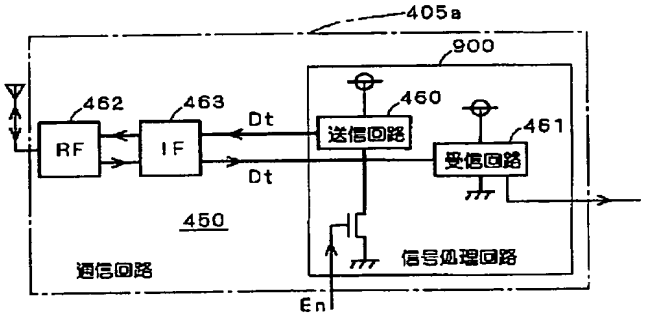
【図６】



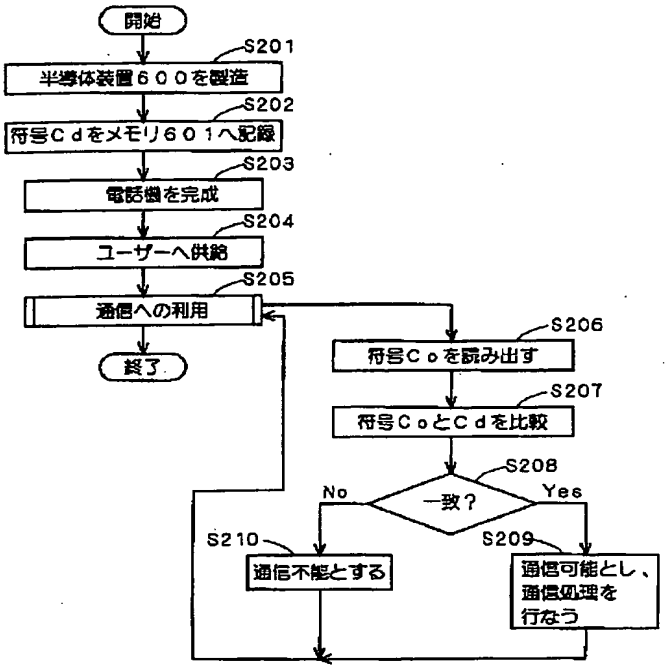
【図９】



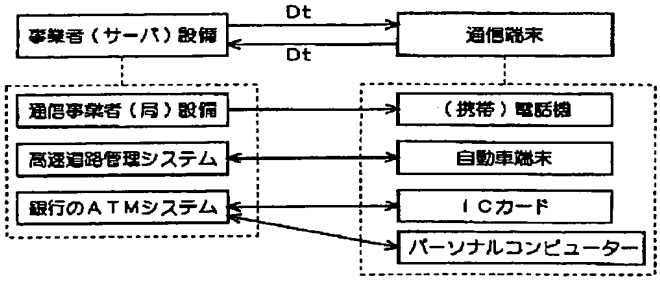
【図１０】



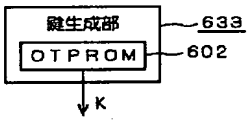
【図１１】



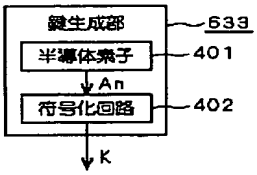
【図１２】



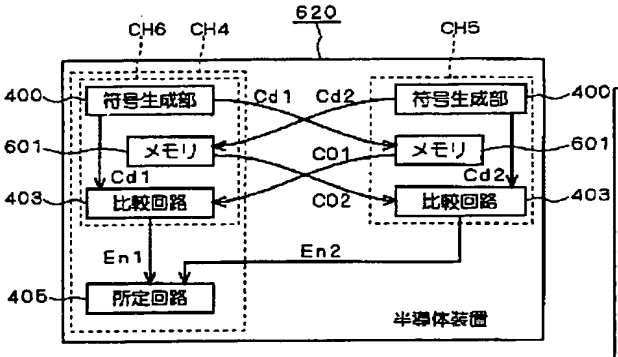
【図２５】



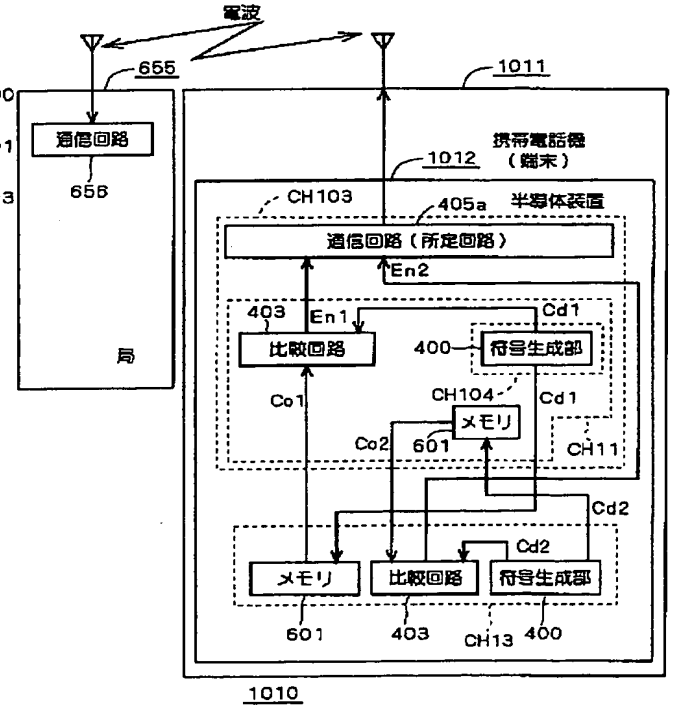
【図２６】



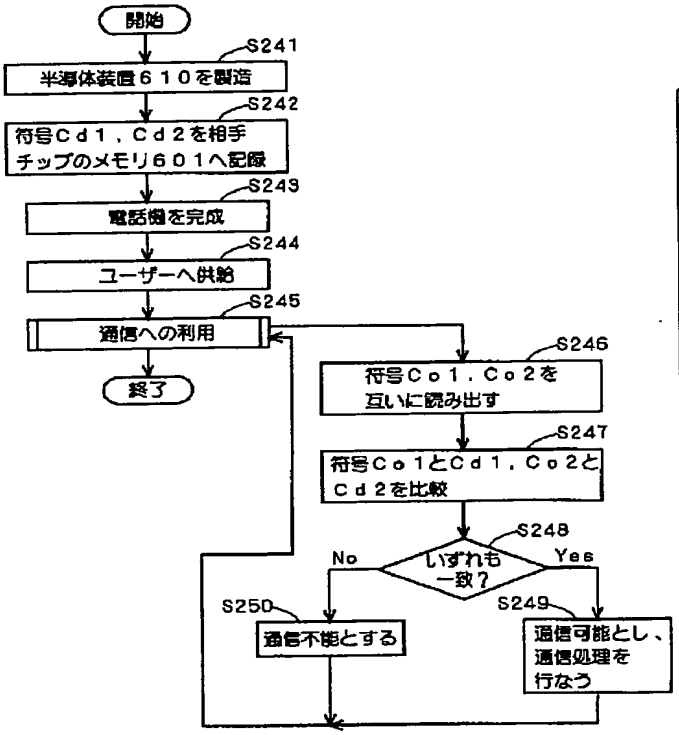
【図１３】



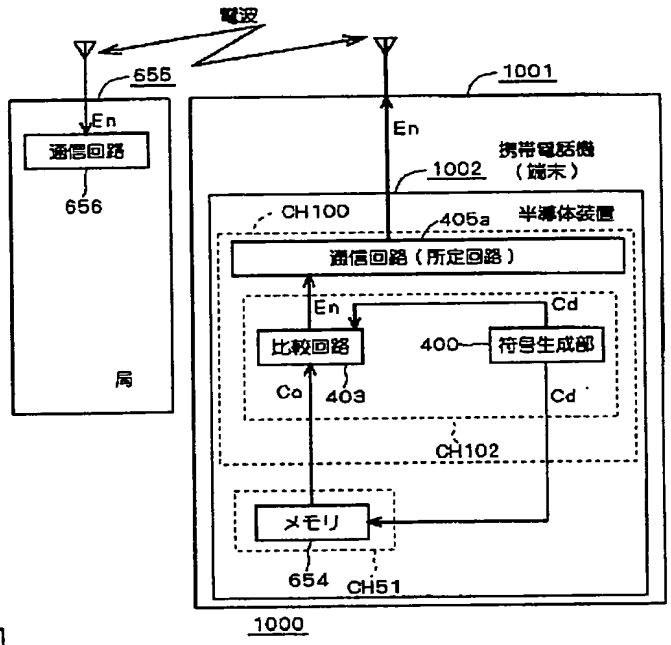
【図１４】



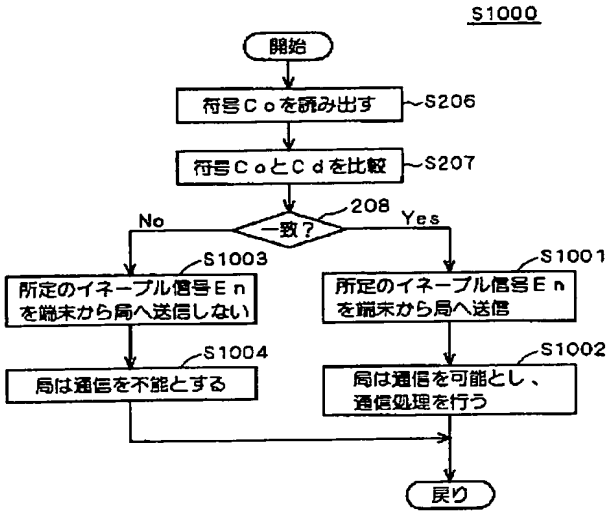
【図１５】



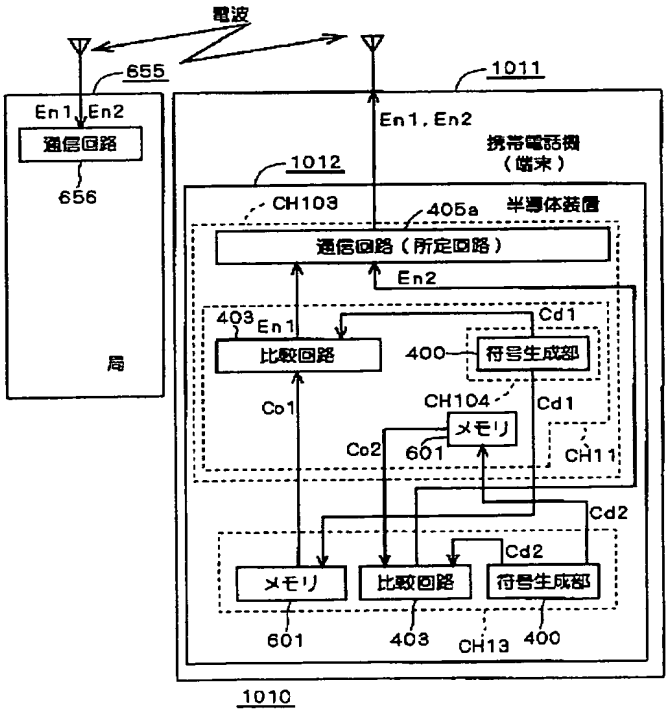
【図１６】



【図１７】



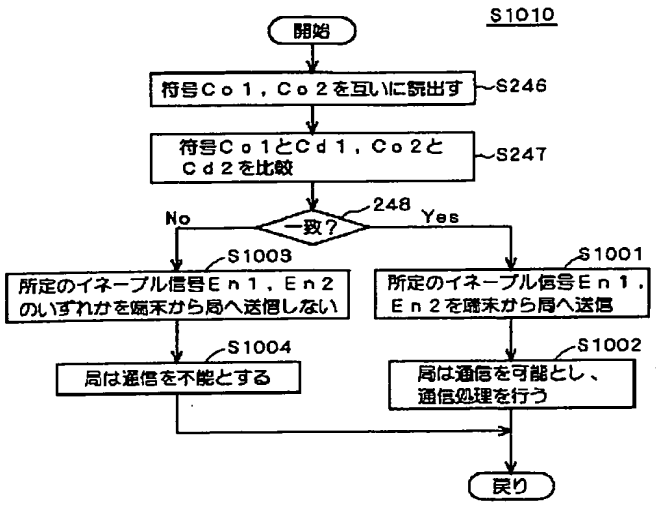
【図１８】



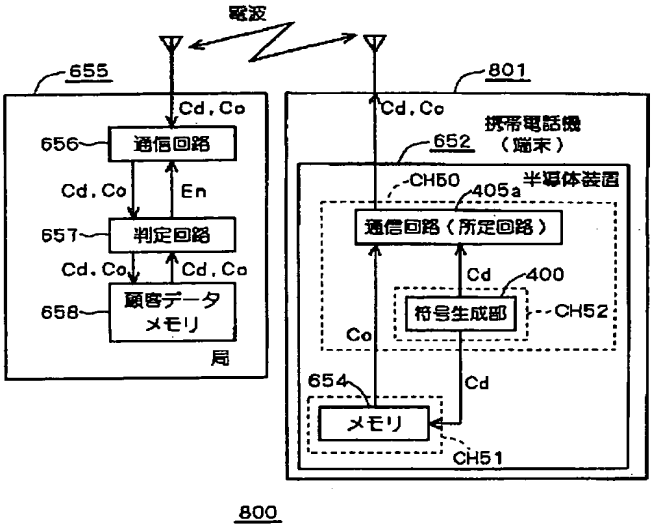
【図５８】

	BL1	BL2	BL3	BL4
WL1	1	1	0	0
WL2	1	0	1	0
WL3	0	0	0	1
WL4	0	1	0	0

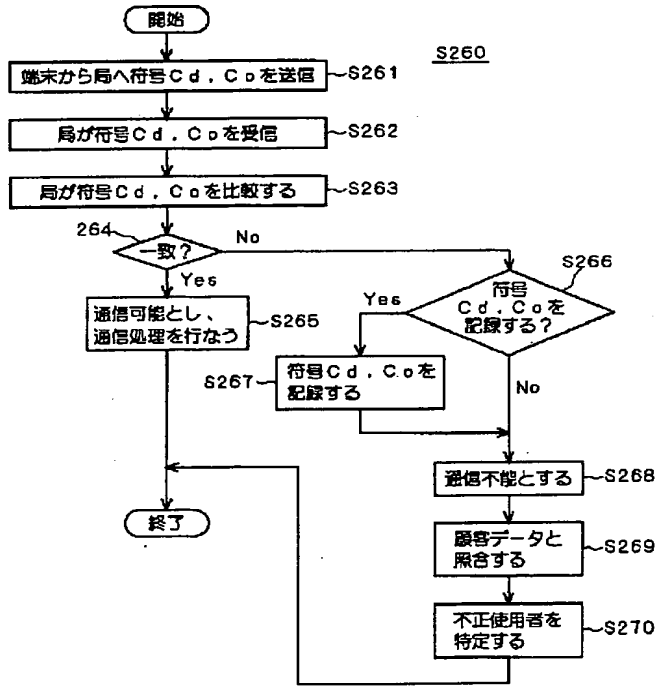
【図１９】



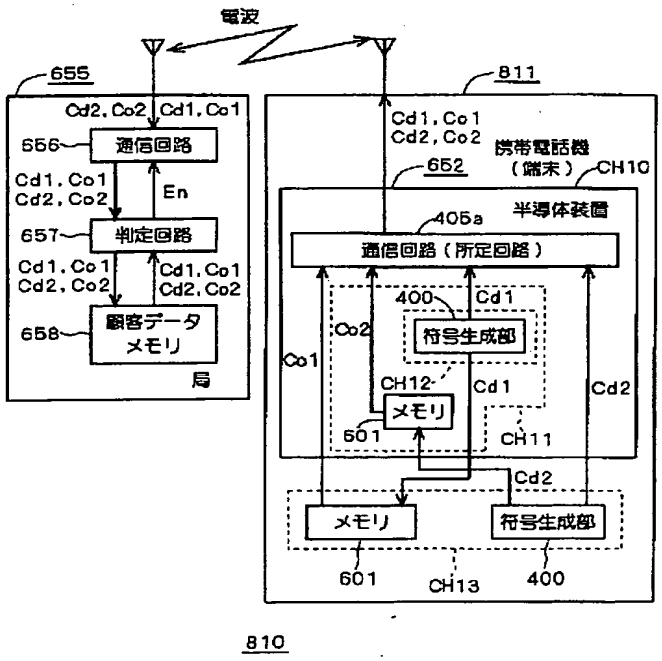
【図２０】



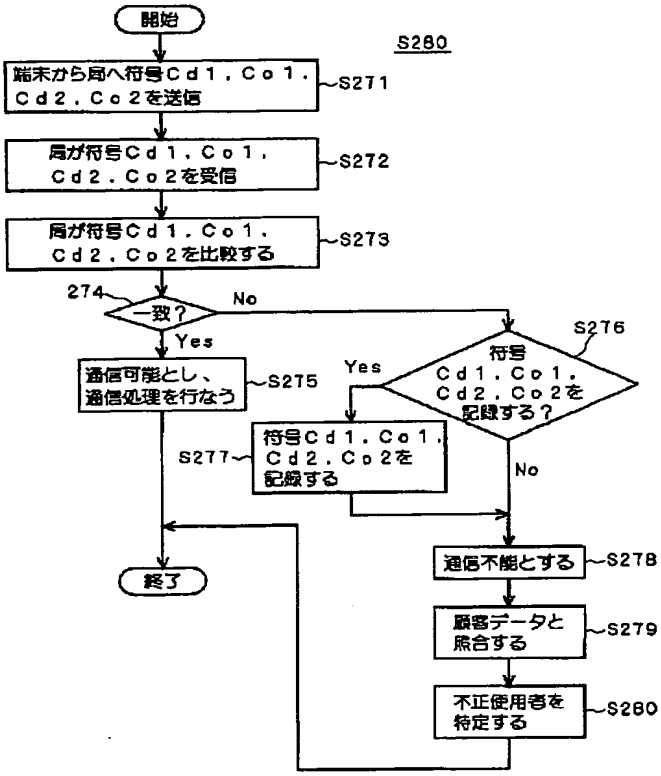
【図２１】



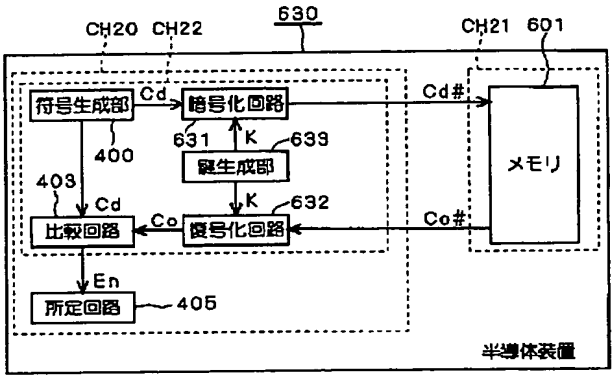
【図２２】



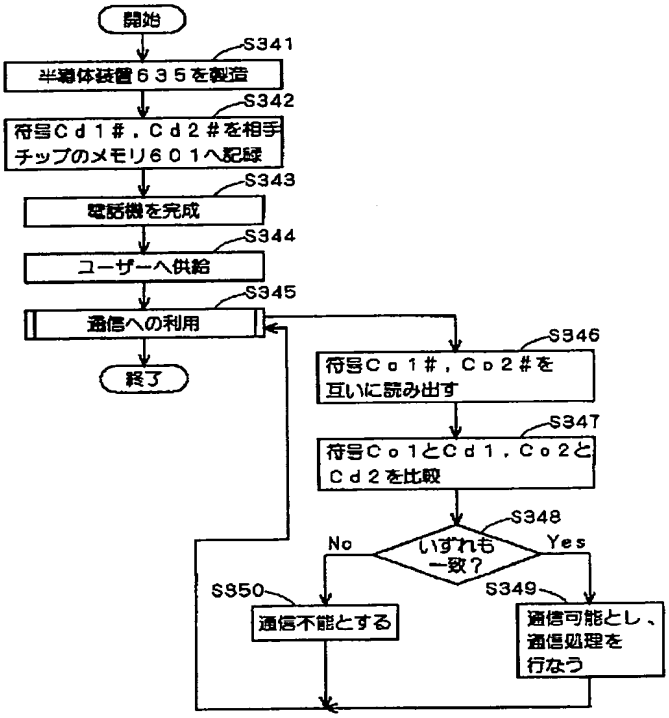
【図２３】



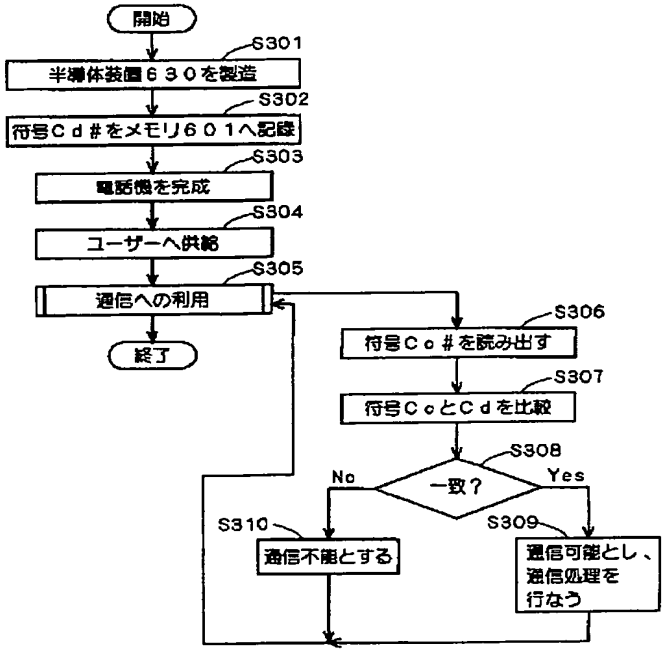
【図２４】



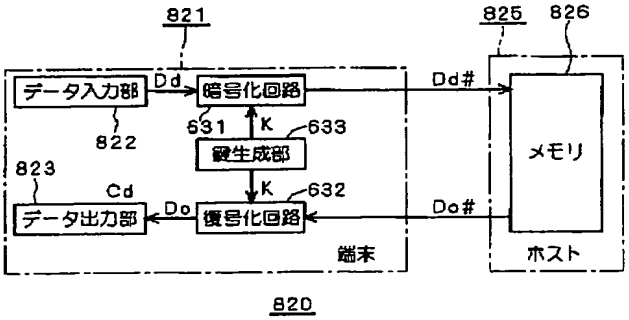
【図２９】



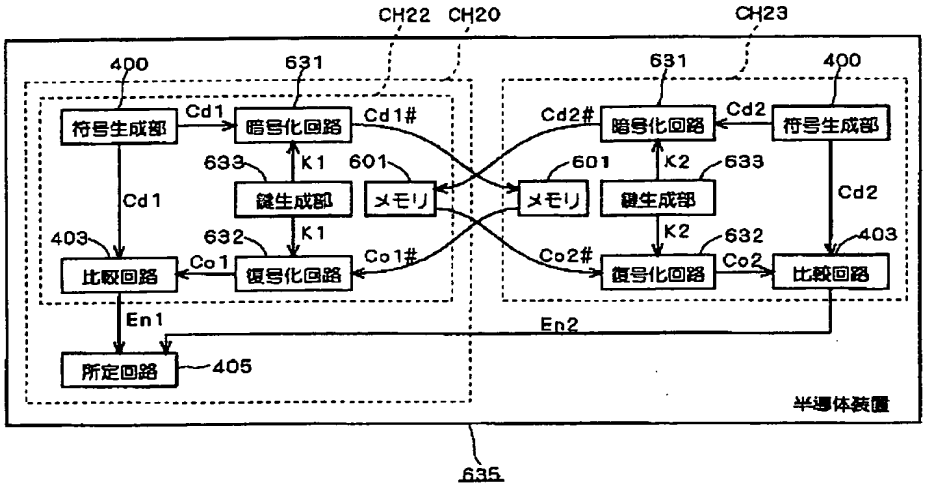
【図２７】



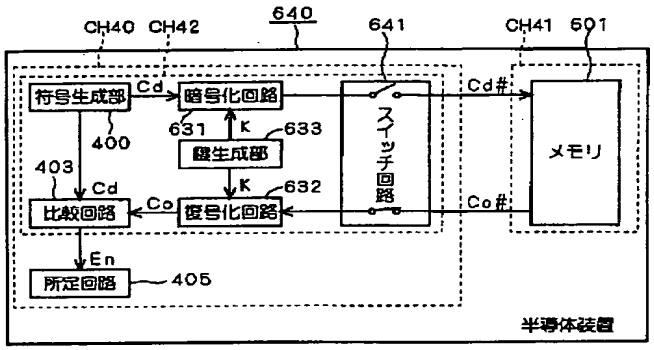
【図３１】



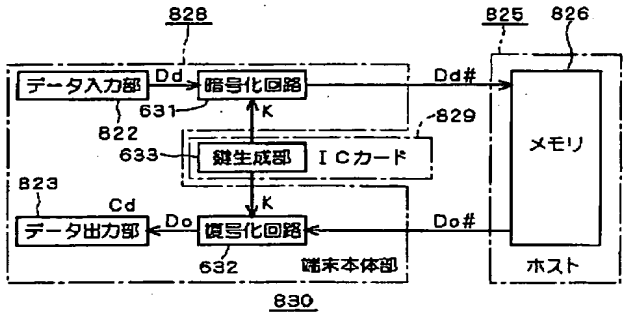
【図２８】



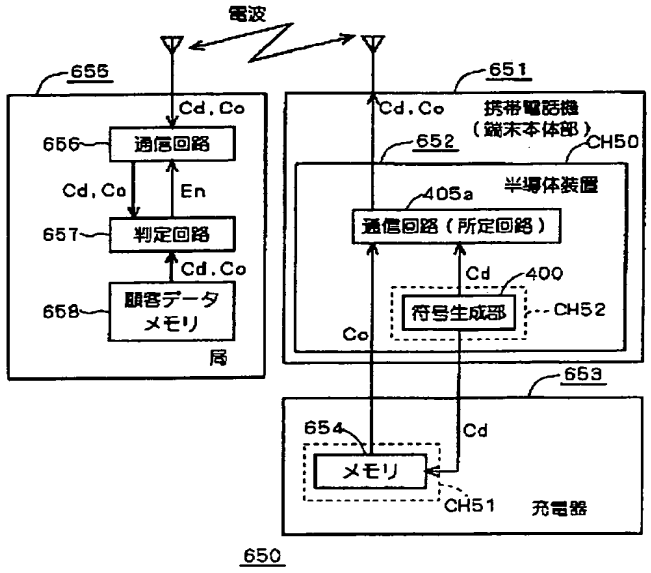
【図３０】



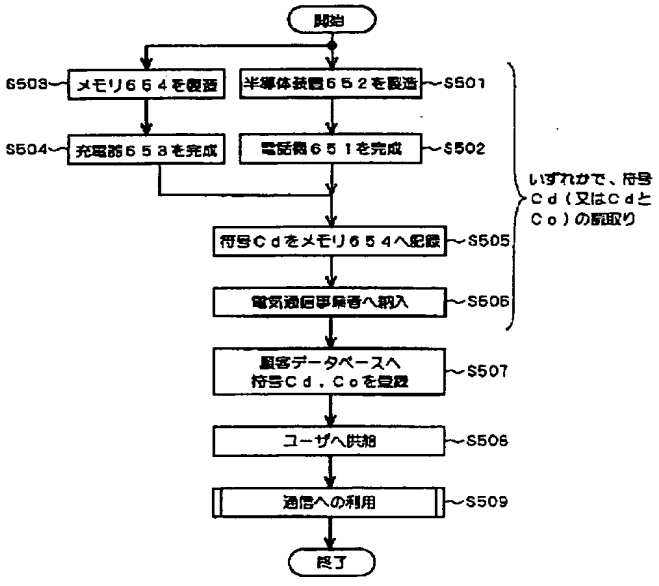
【図３２】



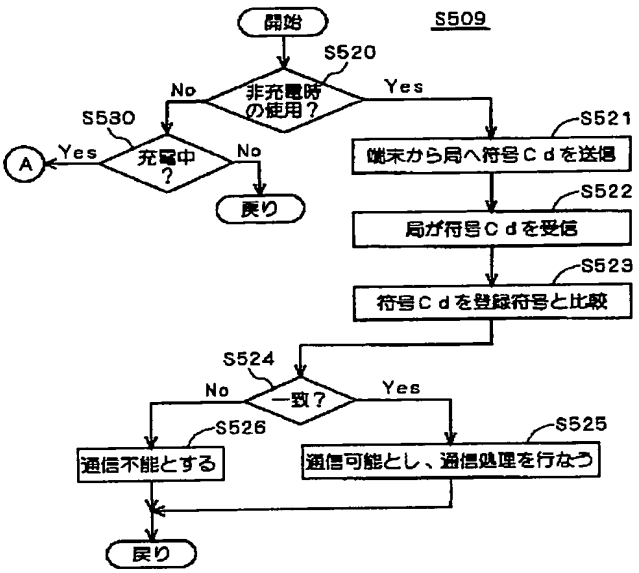
【図３３】



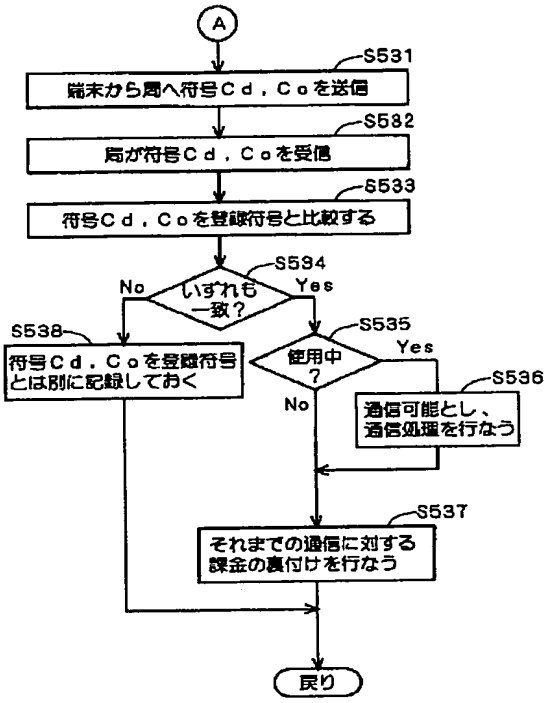
【図３４】



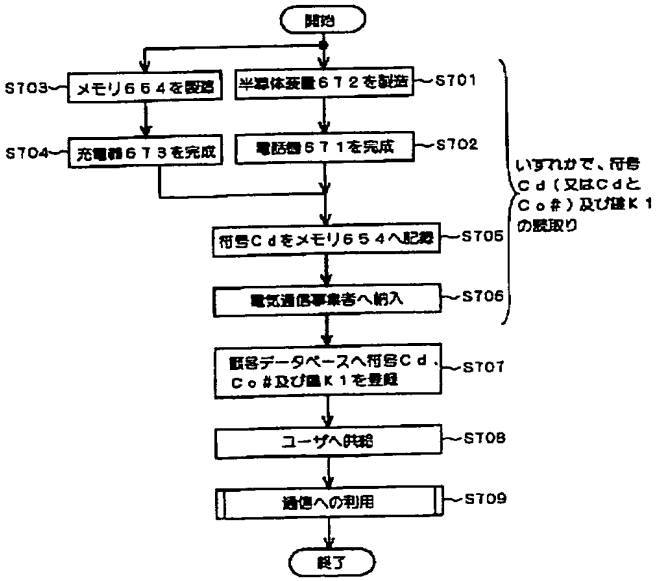
【図３５】



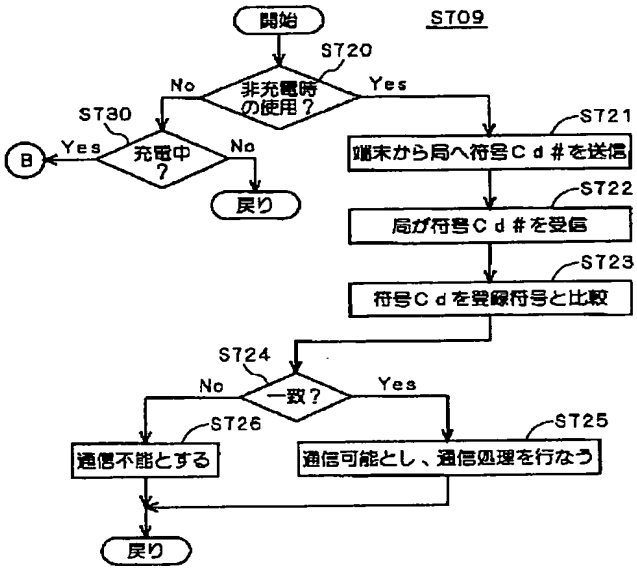
【図３６】



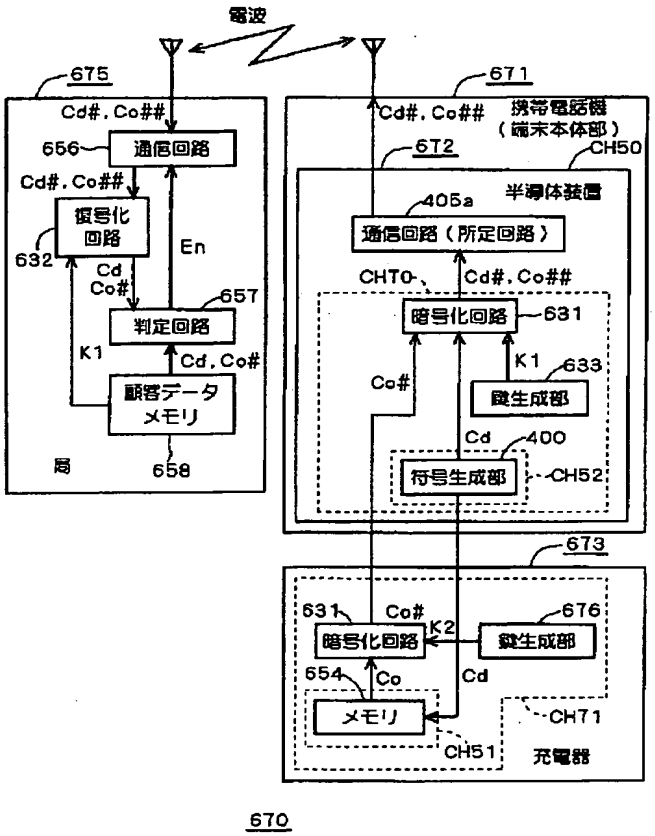
【図３８】



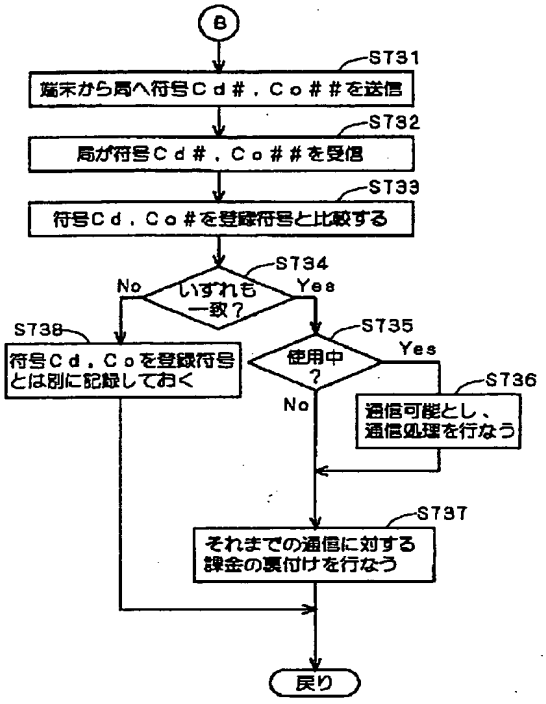
【図３９】



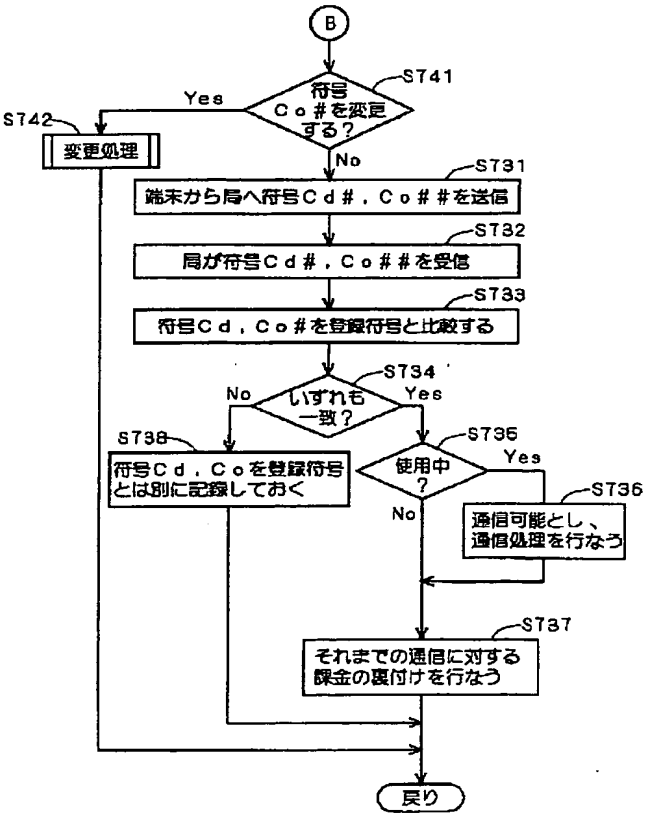
【図３７】



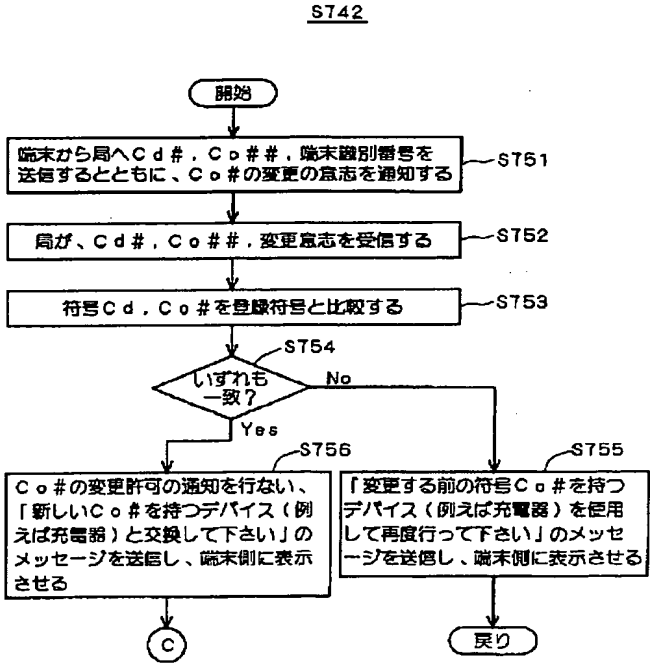
【図４０】



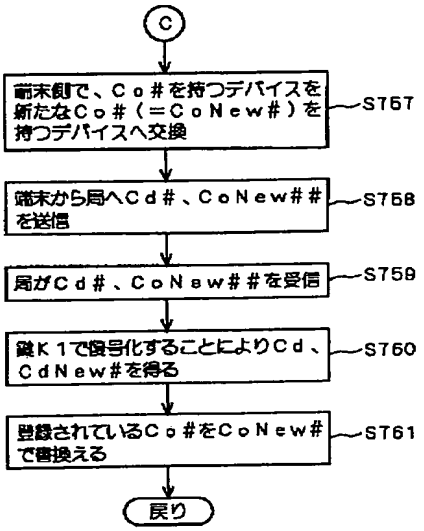
【図４１】



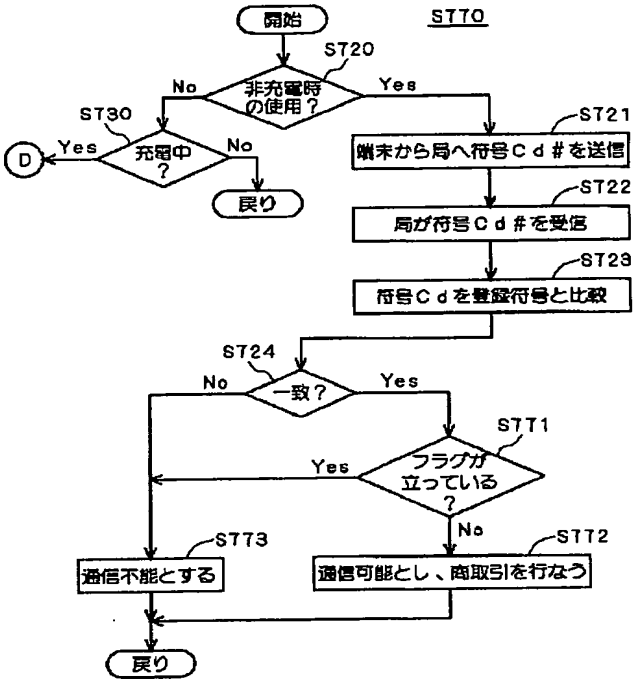
【図４２】



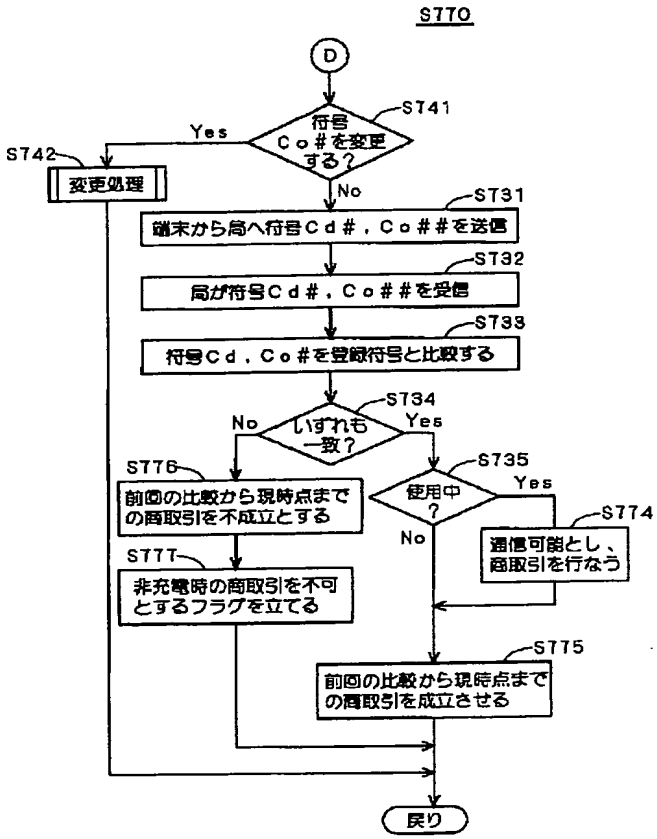
【図４３】



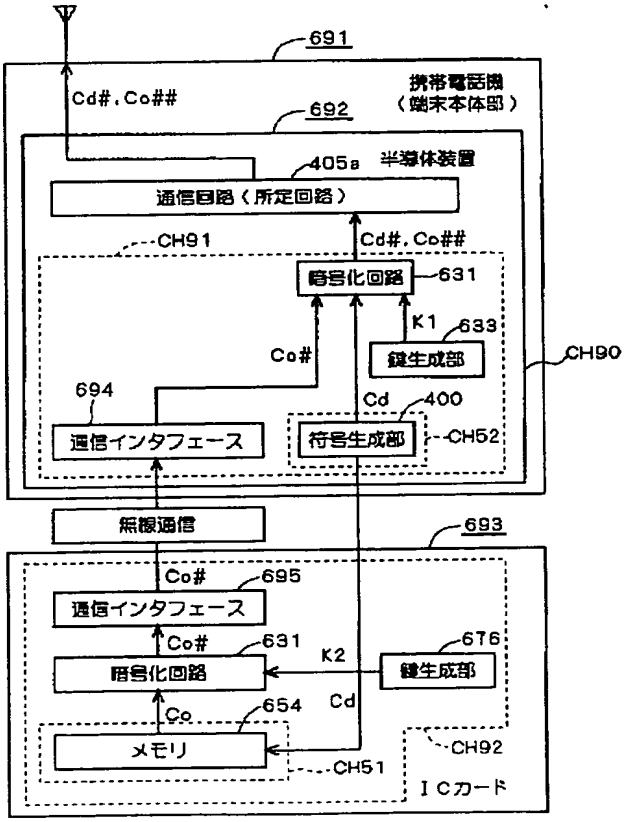
【図４４】



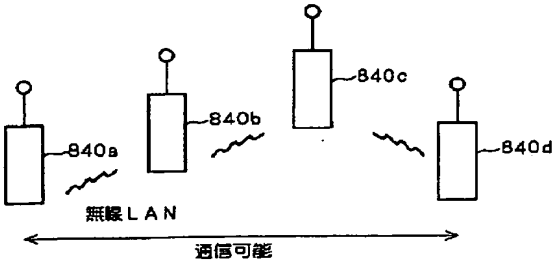
【図４５】



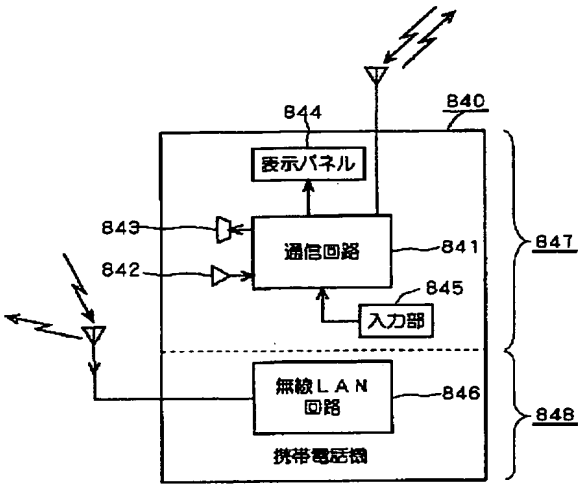
【図４６】



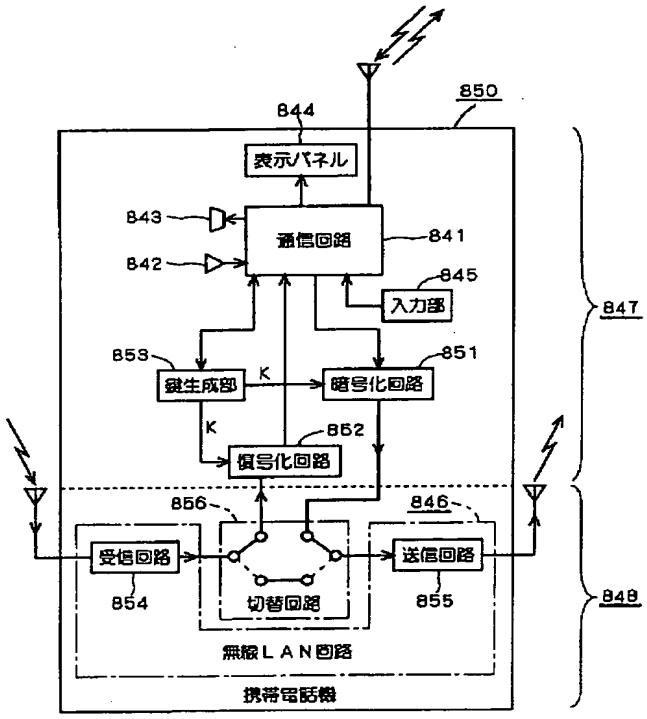
【図４７】



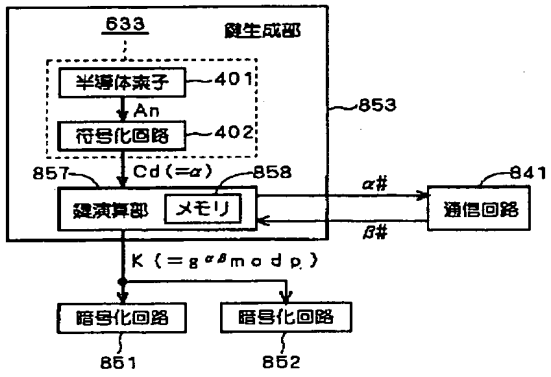
【図４８】



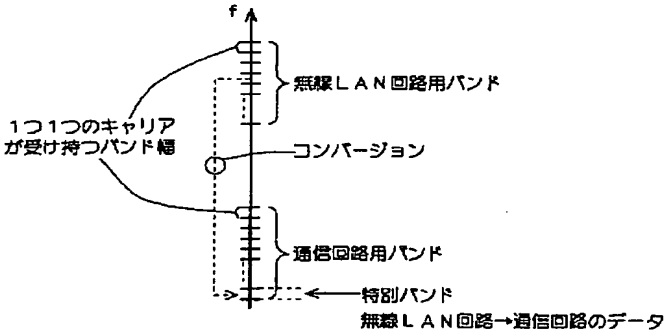
【図４９】



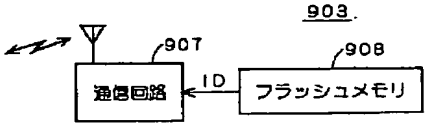
【図５０】



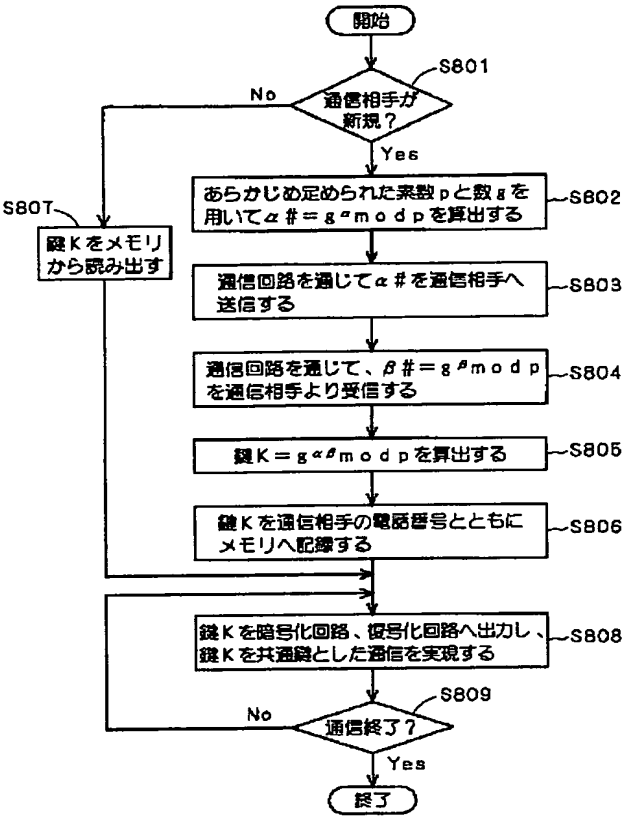
【図５３】



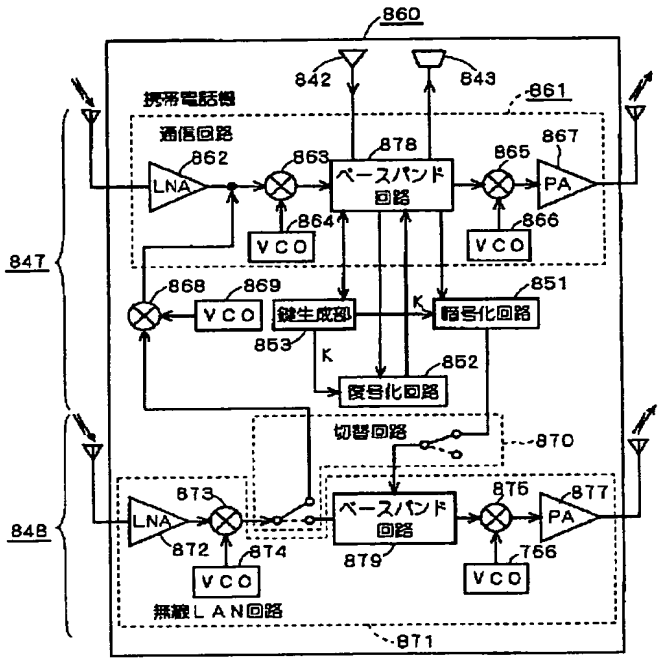
【図６５】



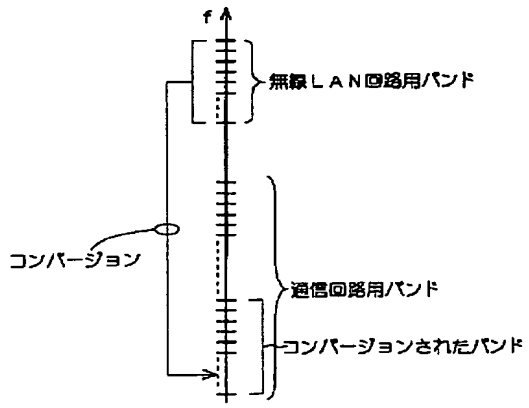
【図５１】



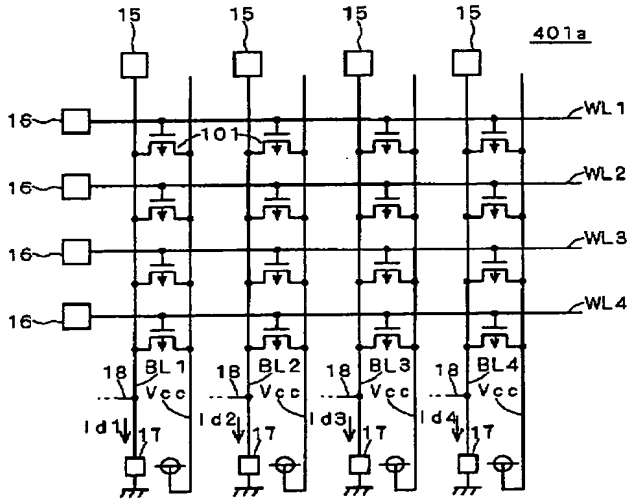
【図５２】



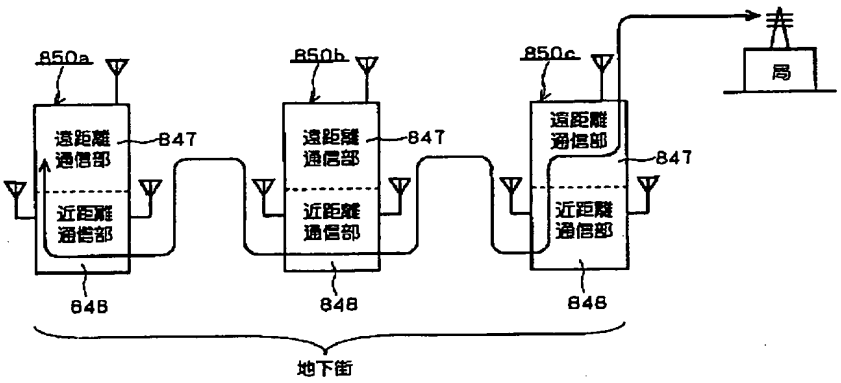
【図５４】



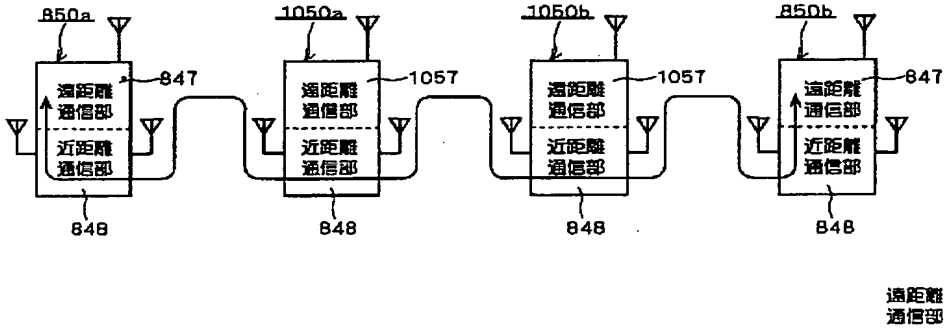
【図５７】



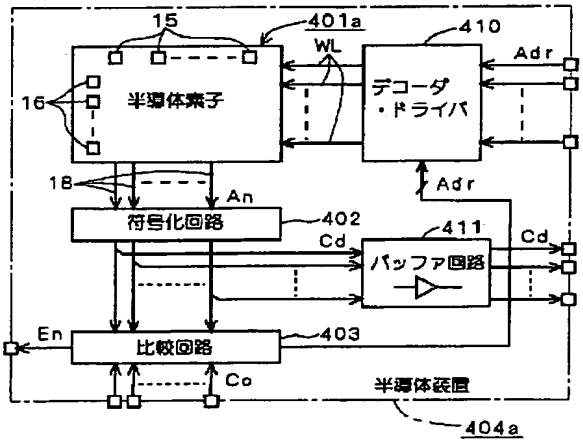
【図５５】



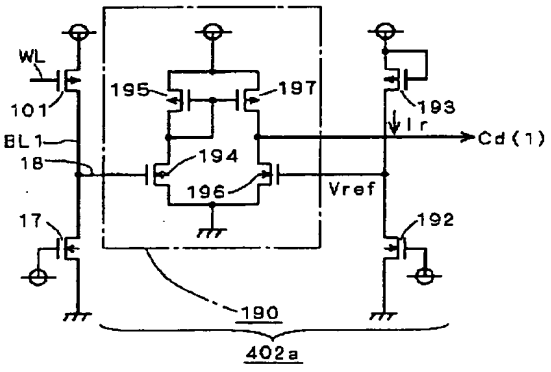
【図５６】



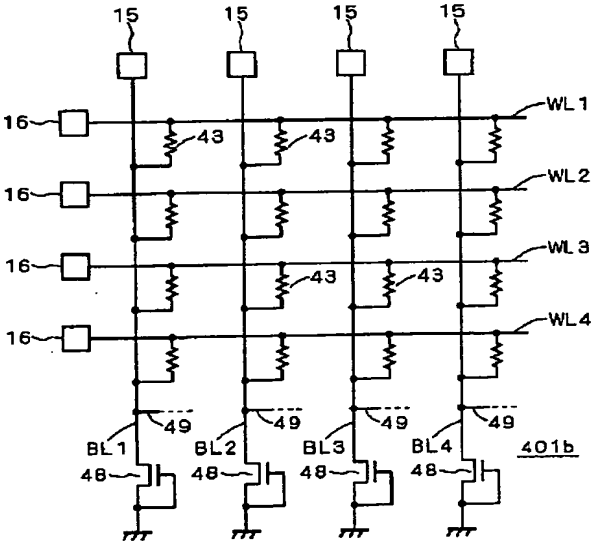
【図５９】



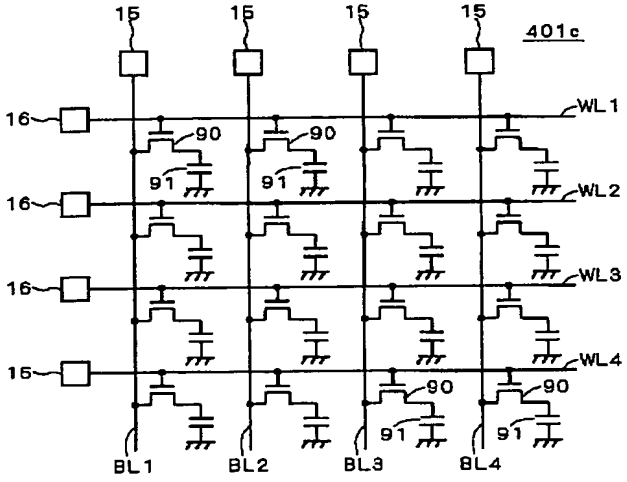
【図６０】



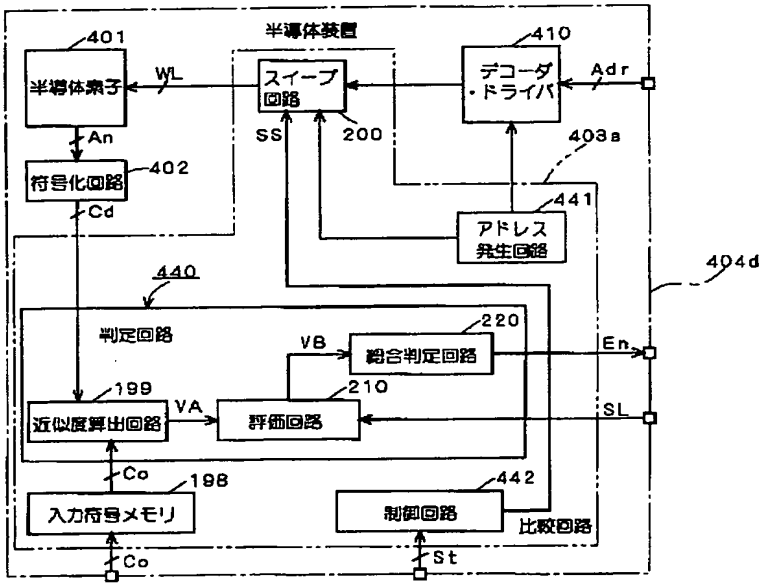
【図６１】



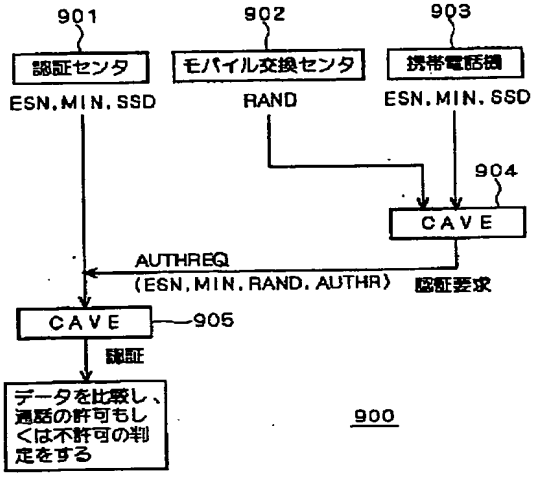
【図６２】



【図６３】



【図６４】



フロントページの続き

(51) Int. Cl.[7]	識別記号	F I	テーマコード（参考）
		H04L 9/00	673C

Ｆターム(参考) 5B017 AA07 BA07 BB03 CA11
5B035 AA13 BB09 BC00 CA38
5B058 CA27 KA02 KA04 KA08 KA33
KA35 YA20
5J104 AA07 KA02 NA02 NA05 NA35
PA02
5K067 AA32 BB04 EE02 EE10 EE16
GG01 GG11 HH05 HH17 HH22
HH23 HH24 HH36